TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technologies

Laura Danilas 212044IVCM

# The Impact of Quantum Technologies on NATO’s Security and Defence Posture

Master's thesis

Supervisor: Adrian Venables<br>PhD

Supervisor: Joanna Śliwa<br>PhD

Tallinn 2024

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Laura Danilas 212044IVCM

# Kvanttehnoloogiate mõju NATO julgeolekule ja kaitsevõimele

Magistritöö

| | |
|---|---|
| Juhendaja: | Adrian Venables |
| | PhD |
| Kaasjuhendaja: | Joanna Śliwa |
| | PhD |

Tallinn 2024

# Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Laura Danilas

12.05.2024

# Abstract

Keeping strategic advantage over any potential adversaries in the world of dynamic and very rapid technology evolution has been a major challenge for NATO lately. Being at the technological edge brings opportunities that can be used in several operational scenarios. Given the current geopolitical situation, NATO has to keep pace with new technologies and plan new ways of warfare by adapting further and faster than ever before, including the field of quantum technologies. In order to gain technological advantage, NATO must be able to integrate quantum technologies into its capabilities and protect against their adversarial use, which is very likely when any conflict occurs. Additionally, current technological advancements are triggered mostly by commercial players, not military players, which is another barrier to the adoption of innovative solutions in the military domain.

This thesis focuses on the impact of quantum technologies on the security and defence capabilities of NATO member states. It provides an overview of the threats and opportunities of quantum technologies and examines how quantum technologies can affect NATO's security and defence posture. This study contributes to a better understanding of the field of quantum technologies, particularly their application in the military domain. In addition, it addresses the issue of quantum technology development as a triangular cooperation between NATO, academia and the industry. Based on the results of the study carried out in the course of the thesis, recommendations are made on how NATO should keep pace with the development of quantum technologies in the 5-, 10- and 20-years timeframe. The results from the research conducted could be taken into consideration by the Allies' policymakers in order to make NATO quantum ready.

This thesis is written in English and is 114 pages long. It includes 8 chapters, 36 figures and 3 tables. It also contains 2 annexes.

Keywords: Quantum technologies, cybersecurity, quantum computing, post-quantum cryptography.

# Annotatsioon

Dünaamilise ja väga kiire tehnoloogia arenguga maailmas on strateegilise eelise säilitamine potentsiaalsete vastaste ees olnud viimasel ajal NATO jaoks suur väljakutse. Tehnoloogilises tipus olemine toob kaasa võimalusi, mida saab kasutada erinevates operatsioonistsenaariumites. Arvestades praegust geopoliitilist olukorda, peab NATO pidama sammu uute tehnoloogiatega ja kavandama uusi sõjapidamise viise, kohandudes kaugemale ja kiiremini kui kunagi varem, sealhulgas kvanttehnoloogiate valdkonnas. Tehnoloogilise eelise saavutamiseks peab NATO suutma integreerida kvanttehnoloogiaid oma võimekusse ja kaitsma end nende kasutamise eest vastaste poolt, mis on konflikti korral väga tõenäoline. Lisaks on praegused tehnoloogilised edusammud enamasti tingitud kommertsettevõtetesest, mitte sõjalistest osapooltest, mis on veel üheks takistuseks uuenduslike lahenduste kasutuselevõtmisel militaarvaldkonnas.

Käesolev magistritöö keskendub kvanttehnoloogiate mõjule NATO liikmesriikide julgeolekus ja kaitsevõimes. Selles antakse ülevaade kvanttehnoloogiate ohtudest ja võimalustest ning uuritakse, kuidas kvanttehnoloogiad võivad mõjutada NATO julgeolekut ja kaitsevõimet. See uuring aitab kaasa kvanttehnoloogiate valdkonna paremale mõistmisele, eelkõige nende rakendamisele militaarvaldkonnas. Lisaks käsitletakse kvanttehnoloogiate arendamist kui kolmepoolset koostööd NATO, akadeemiliste ringkondade ja tööstuse vahel. Magistritöö käigus läbiviidud uuringu tulemuste põhjal antakse soovitusi, kuidas peaks NATO sammu pidama kvanttehnoloogiate arenguga 5, 10 ja 20 aasta perspektiivis. Läbiviidud uuringu tulemusi võiksid arvesse võtta liitlaste poliitikakujundajad, et NATO kvanttehnoloogiate tuleku jaoks valmis oleks.

Lõputöö on kirjutatud inglise keeles ning on 114 lehekülge pikk. See sisaldab 8 peatükki, 36 joonist, 3 tabelit. Sellel on ka 2 lisa.

Märksõnad: Kvanttehnoloogiad, küberkaitse, kvantarvutused, postkvantkrüptograafia.

# Acknowledgements

First and foremost, I would like to thank my supervisors, Dr Adrian Venables and Dr Joanna Sliwa, for their contribution and continuous support. Without their professionalism, expertise, motivation and knowledge, I wouldn’t be able to write this thesis. I want to thank Dr Venables, who helped me with academic writing and research design. My heartfelt thanks go to Dr Sliwa, whose immense expertise, patience and commitment inspire me every day. I feel so honoured to have had the opportunity to work with both of them, with great reverence to them.

I am so grateful from the bottom of my heart for the opportunity that I was given to work as an intern for NATO Cyber Security Centre, Capability Development (CAPDEV) branch in particular. I am thankful that I got to write this thesis as part of my internship, and I feel so happy that I got to create something that really matters, especially regarding the current geopolitical situation. I believe that this work I have done will live on even after the internship.

I would like to express my sincere gratitude to my colleagues at the NATO Communications and Information Agency (NCIA) in The Hague. Seeing them and working with them every single day gave me an opportunity to develop my skills personally and professionally. From day one, I felt that I belonged to a family.

I would like to thank all the experts who took part in my research. With your support, feedback and insightful comments this thesis wouldn't be written. I am thankful for those who took some time to have an interview or discussion with me.

This MSc thesis is dedicated to my family and friends who supported me throughout my studies.

# List of abbreviations and terms

| | |
|---|---|
| AI | Artificial Intelligence |
| BHE | Biotechnology and Human Enhancement |
| CIS | Communications and Information Systems |
| CoE | Centre of Excellence |
| CRM | Critical Raw Materials |
| CRQC | Cryptographically Relevant Quantum Computer |
| EDF | European Defence Fund |
| EDTs | Emerging Disruptive Technologies |
| ESA | European Space Agency |
| EU | European Union |
| FTQC | Fault-Tolerant Quantum Computer |
| HNDL | Harvest now, decrypt later |
| IT | Information Technology |
| JCIDS | The Joint Capabilities Integration Development System |
| JISR | Joint Intelligence, Surveillance and Reconnaissance |
| NATO | North Atlantic Treaty Organisation |
| NISQ | Noisy Intermediate-Scale Quantum |
| NIST | National Institute of Standards and Technology |
| NMM | Novel Materials and Manufacturing |
| PKI | Public Key Infrastructure |
| PQC | Post-Quantum Cryptography |
| QC | Quantum Computing |
| QEC | Quantum Error Correction |
| QIS | Quantum Information Science |
| QKD | Quantum Key Distribution |
| QML | Quantum Machine Learning |
| QR | Quantum Resistance |
| QRAM | Quantum Random Access Memory |
| QRNG | Quantum Random Number Generator |
| QT | Quantum Technologies |
| R&D | Research and Development |

|  |  |
|---|---|
| SNDL | Store now, decrypt later |
| STANAG | NATO Standardization Agreement |
| STO | NATO Science and Technology Organisation |
| TRL | Technology Readiness Level |
| US | The United States of America |

# Table of contents

# List of Figures

# List of Tables

# 1 Introduction

The development of information technology has been characterised by continual and rapid changes. This is particularly so in the field of Quantum Technologies (QT). The development of quantum mechanics began with Max Planck in the 1930s when he theorised the energy distribution of light. At this time, quantum mechanics was a revolutionary theory and most of the scientific community, including Albert Einstein, was reluctant to accept it [1]. QT do not bring us new weapons or standalone military systems. QT are here to enhance measurement capabilities, computation, efficiency and precision power of future and current technologies [2].

The race between superpowers and leading technology companies to achieve an advantage in developing QT has joined cyber-physical systems (Industry 4.0) and artificial intelligence as key growth areas. The first quantum revolution began around 1900 with the birth of Max Planck's quantum hypothesis. The second quantum revolution started in the 1980s and lasted until the beginning of the 21st century. It can be argued that the world is currently undergoing a third quantum revolution, which includes the real-world deployment of quantum computers [3]. The first commercially available quantum computer was introduced by the company D-Wave Sytems in 2011 [4]. If the quantum revolution grows at the same pace as in the field of artificial intelligence, significant societal and economic changes can be expected [3].

In 2020, the NATO[1] Science and Technology Organization (STO) defined eight "major strategic disruptors" relevant to NATO's capabilities between 2020 and 2040 [5]. These are data, artificial intelligence (AI), autonomy, space technologies, hypersonics,

[1] The North Atlantic Treaty Organization (NATO), founded in 1949, currently (in 2024) consists of 32 member states, which are independently building their military capabilities. However, the Alliance is founded on the principle of collective defence. According to NATO's Article 5, if one NATO Ally is attacked, then all NATO Allies are attacked. Whenever NATO carries out a mission, member states commit troops and equipment to be part of the NATO forces. This is possible with employment of NATO's Command Structure, where military and civilian personnel from all member states work together [6]. In this thesis, the term "NATO" is understood as an Alliance of 32 member states and used interchangeably with the term "Alliance".

biotechnology and human enhancement (BHE), novel materials and manufacturing (NMM) and QT. NATO has identified quantum as a key emerging technology whose potential applications might enable allies to enhance its warfighting capabilities [7]. More importantly, QT can also degrade the Alliance's ability to defend and deter [8]. NATO Allies have also prioritized quantum as one of the technological areas due to its implications for security and defence [9].

Over the last few decades, this technology has rapidly evolved. Public and private investments totalled $35.5 billion by 2022 across a range of QT [10]. Governments and private companies, such as Google and Amazon, have spent hundreds of millions of dollars in research and development [7]. This is also true of adversarial governments, such as China, which launched the world's first quantum satellite "Micius" in 2016 [11]. The satellite reached a new milestone by establishing an ultrasecure link between two ground stations, and thus, a secure method of quantum messaging was introduced. This is one more step towards truly unhackable global communications.

QT are being developed for many civilian applications, and the military also considers it as potentially game-changing, especially in information and space warfare. Although Technology Readiness Levels (TRL) vary, there is clear evidence that QT will have increasingly important strategic and operational implications for NATO across all domains of operation. Emerging work in this field will increase in significance and importance as NATO seeks to capitalize on QT. NATO has the potential to become a leader in this field by using its testing and validation infrastructure, including test centres and access to end-user military operations [7]. However, it is believed that quantum computers, when finally built, will be able to break current public-key cryptography [12]. This capability can be perceived as both a strategic opportunity and a threat.

NATO introduced its first ever quantum strategy in January 2024 [9]. The aim of the strategy is to outline the possibilities of how quantum can be applied to security and defence and to share a strategic vision – to become a quantum-ready alliance. The quantum strategy does not mean that NATO is ready for the upcoming and ongoing quantum revolution, but it will help NATO to take next steps towards it. It is clearly seen that today's actions need to be aligned with tomorrow's risk landscape.

This thesis investigates the role of QT within the context of NATO’s security and defence posture. In particular, it highlights their impact within the cyberspace[1] [13] domain and finds out what are the weaknesses that can restrict the application of QT in military operations.

## 1.1 Motivation

Of all the Emerging and Disruptive Technologies (EDTs) identified as priority areas for NATO, QT are the most nascent and variable in development, with substantial commercial and national investments already being made [14]. NATO has already started to work on QT and understand its implications for the Alliance’s core tasks, taking into account that QT are the first EDTs that have its own strategy. At the 2021 NATO Summit, the leaders of NATO agreed with the NATO 2030 Agenda [15]. This framework is a transatlantic initiative for NATO’s future, strengthening and protecting the Alliance by remaining ready today to face tomorrow’s challenges [15]. One of the key points of this document is the necessity to preserve NATO’s technological edge. With this agenda, NATO Allies agreed to launch a new civil-military Defence Innovation Accelerator for the North Atlantic (DIANA) [16], but also establish a multi-nationally funded NATO Innovation Fund [17]. This initiative was created to build accelerators and promote local investments in QT development in NATO countries.

The first tangible impact of QT on NATO’s Information Technology (IT) infrastructure is related to the compromise of the public key cryptography algorithms (e.g. used for keys’ generation and negotiation). This so-called quantum threat is real already now, because the traffic can be collected before a cryptographically relevant quantum computer (CRQC) is built. These are called Harvest Now, Decrypt Later (HNDL) attacks [18]. In May 2022, the president of the US, Joe Biden, announced a memorandum and an executive order to address the quantum threat by 2035 [19] [20]. Therefore, NATO and

[1] In 2021, at the NATO Summit in Brussels, NATO Allies endorsed its Comprehensive Cyber Defence Policy, emphasising its core tasks: protect its own networks, operate in cyberspace, help Allies to enhance their national resilience and provide a platform for political consultation and collective action as well as its overall deterrence and defence posture. At the 2023 NATO Summit in Vilnius, the Allies launched NATO's Virtual Cyber Incident Support Capability (VCISC) to support national mitigation efforts in response to significant malicious cyber activities.

its Allies must be quantum ready. What exactly does it mean? This will be answered in this thesis with respect to cybersecurity.

In order to become quantum-ready in the next 10 years, therefore NATO and its Allies must make concerted efforts. These are important to foster QT systematically through accelerating development and adoption while protecting our quantum ecosystems from licit and illicit acquisitions by the Alliance's strategic competitors and potential adversaries. NATO leads the discussion on QT in defence and security, helping to continuously build on a shared understanding and leveraging QT potential while safeguarding against its adversarial use. The interaction, combination, interdependency and synergy between QT and other EDTs – such as AI, Data, Autonomy, Space, and Biotechnology – will transform security and defence, as well as industry, over the next 20 years. QT is potentially a game changer for future military operational environments. Although still in the early stages of development, it is rapidly evolving, simultaneously increasing the technical and knowledge potential of the industry and the states that invest in it.

The motivation for this thesis comes from the NATO 2030 initiative. NATO has stated that it wants to preserve its technological edge, which includes the application of game-changing QT. Many Allies have already started developing national strategies and undertaking initiatives to implement QT. But it is clearly seen that the opportunities of QT come with threats. This thesis is written in order to support the strategic decision-making process targeted towards planning necessary actions to accelerate the adoption of QT in support of NATO's security and defence posture.

## 1.2 Research Purpose

The purpose of this thesis is to analyse the impact of QT on the security and defence posture of NATO and its member states, as well as potential military operations. This will result in a series of recommendations as to what the member states and NATO should do in order to maximize the benefits and mitigate the threats of QT.

## 1.3 Research Questions

In order to start with the research and find out the best methodology for the research, three research questions were posed. The research methodology is described in Chapter 3. This thesis addresses a significant research gap by using scientific methods to investigate the potential challenges and opportunities of QT application in military domain within the context of cybersecurity.

In order to address the main research purpose of the thesis, which is the impact of QT on NATO’s security and defence posture, the following research questions are answered:

**RQ1.** What QT are seen as threats and opportunities to NATO's cybersecurity, and how can they influence the security posture of NATO’s communications and information systems (CIS)?

**RQ2.** What should NATO do in order to support the development of QT for military applications to protect the Alliance?

**RQ3.** What are the indicators that could guarantee NATO quantum readiness?

## 1.4 Target Audience

The thesis is targeted towards military leaders of Allied NATO member states to understand:

- the urgency of focusing on the technologies at stake, whose impact cannot be predicted with full confidence in this moment, and
- the collective responsibility to engage in the process of their development for the benefit of the Alliance.

## 1.5 Scope and Goal

The research is limited to open-source material and unclassified documents. This study is based on publicly available sources of information, mainly scientific publications, books and articles that offer the most recent and advanced knowledge of the matter.

## 1.6 Novelty

The literature review presented in Chapter 2 finished with the conclusion that the biggest research gaps occur from academic sources that cover quantum topics from both military and cybersecurity perspectives. This is especially important when strategic decisions need to be made by engaging People, Processes and Technology (PPT framework) in order to plan the path towards the application of QT in security and defence [21]. Only a few research papers have been published on this topic, especially considering NATO and its capabilities. Research papers usually consider theoretical, laboratory work, or commercial applications of quantum technologies. However, there is still a lack of credible references focusing on what being quantum ready means for the Alliance and how this should be approached. In addition, since some of NATO’s papers and documents are classified, they cannot be used as references for academic research. Sources for this thesis will include government publications, existing academic material and other documents. The novelty of this thesis is that this level and depth of research has not previously been undertaken, particularly investigating QT in the military domain within NATO member states. The impact of QT on cybersecurity and NATO’s military operations has not been studied in this form and on this scale.

## 1.7 Chapter Overview

Chapter 2 is dedicated to describing and explaining the topic of QT through a literature review. The chapter provides an introduction to existing QT and their state of the art. Additionally, this chapter presents some important definitions that will be used throughout the thesis. The second part of the chapter examines QT from the perspective of their influence on NATO's cybersecurity. The chapter concludes with an overview of global players in QT.

Chapter 3 provides an overview of the methodology used in this research. A survey based on the Delphi method was created and used to answer the RQs. The main aim of the survey was to gather insights from quantum experts by requesting them to evaluate various statements on the Likert scale. This chapter is dedicated to analysing diverse aspects in the development and implementation of QT. Ethical considerations and validation of methods can be also found in this chapter.

Chapter 4 serves as a section for presenting the results of the research. The results collected from the survey were assessed in this chapter. The quantitative analysis provides an overview of QT experts based on their experience and perceptions.

Chapter 5 begins with 10 main findings that emerged from the research. The chapter continues with an analysis of the results statement by statement.

Chapter 6 focuses on the discussion. The results of the survey are combined with two main topics of this chapter – a discussion of the main findings and a discussion of the RQs. Chapter 7 presents some ideas for future research.

Chapter 8 summarises the findings, emphasizing the main takeaways from this research and the conclusions that can be drawn. This chapter also includes a table of recommendations.

# 2 Literature review

The chapter aims to explain the theoretical background of the topic by conducting an in-depth analysis of published studies and articles in the field of QT with a focus on cybersecurity. It starts by reviewing various papers and publications that shed light on the rising significance of QT, especially within military operations. While there is a wealth of publications on the advancements of quantum technologies in different countries, research on their link to military domains, particularly in a NATO context, is not as prevalent. However, NATO, along with renowned defence organizations, international affairs institutes, and scientific journals, has produced numerous papers which this research will reference.

For this study, a variety of resources were utilized, including books, blogs, conference and research papers, workshop materials, articles, publications, and reports. To lay the groundwork for this research, NATO restricted materials such as strategic documents were consulted. However, only open-source and publicly available materials were referenced and analysed. When analysing the theoretical aspects, older sources were consulted, while newer references were employed for practical applications due to the rapid development of QT and the potential obsolescence of information and applications. The author critically evaluated the value of these resources and opted to use materials authored by well-known and highly regarded experts in quantum science. The resources were limited to those available in English and Estonian.

## 2.1 Quantum Technologies

QT are an emergent and disruptive discipline, that can affect many human activities [2]. As with all digital technologies, QT are neither good nor bad; they can be used for both malicious and virtuous purposes. According to the NATO Science and Technology Organisation (STO), QT are generally grouped into three broad overlapping categories – quantum computing, quantum communication, and quantum sensing [22]. These three sub-fields possess potential applications and capabilities that will influence all domains[1] of warfare in the future. In this thesis, the focus is put on quantum communication and quantum computing as the whole analysis part is performed from the cybersecurity perspective, and these two are the most relevant ones. Opting out quantum sensing was not caused by its irrelevance to NATO. On the contrary, they are seen as interesting for NATO missions with respect to the Joint Intelligence, Surveillance, Reconnaissance (JISR). However, their relevance to the cybersecurity dimension is limited.

### 2.1.1 Fundamental Principles of Quantum Mechanics

This subchapter gives an overview of the basic defining principles of quantum mechanics necessary to understand the following chapters.

According to the STO definition, *Next-generation quantum technologies exploit quantum physics and associated phenomena at the atomic and sub-atomic scale, particularly quantum entanglement and superposition* [22]. These basic quantum phenomena are:

- a state of **superposition** – A quantum system can exist in two or more states at the same time [23]. In the explanation of superposition, a parallel with flipping a coin can be drawn. By flipping a coin, it will fall on either one side or another, but by spinning a coin, its dimensional possibilities increase exponentially [24]. These groups of qubits that are in superposition are able to create complex and multidimensional computational spaces. Quantum computers can work by preparing a superposition of all possible computational states [25].
- **quantum entanglement –** A strong correlation between two or more particles that have no corresponding classical analogue comparison [23]. The bond among these objects is very peculiar and has an important property. Changing the state of one member of an entangled collection causes a change in the state of the other objects in the group [26].
- **no-cloning** theorem means, that state of a particle cannot be copied. It has profound consequences for qubit error correction and for quantum communication security (see Chapter 2.1.4) [27]. As the theorem explains, due to the fact that a

[1] NATO Multi-Domain concept of operations (MDO) states that NATO operates in five domains combined together – air, space, land, sea, and cyberspace, which provide a vehicle for enhanced deterrence and defense [28].

qubit is fragile and cannot be copied, this makes the error correction of qubits much more complicated [2].

- **coherence** – is the ability of a quantum state to maintain its superposition and entanglement in the face of interactions [29]. Coherence decays with time, when a quantum system is in contact with its environment. This process is called quantum decoherence [1]. Decoherence can be viewed as a loss of information from a system into the environment, one of the examples why it can happen are cosmic waves [30].

### 2.1.2 Quantum Computing

Quantum computing was initially proposed by physicist and Nobel laureate Richard Feynman already in 1982 [31]. In the context of NATO, quantum computing is considered the potentially most disruptive QT of all if successfully deployed [22]. A quantum computer is a computing device that stores information in qubits and transforms them by exploiting very specific properties of quantum superposition, entanglement, and coherence effects within systems governed by such quantum mechanical effects [32]. Quantum computers utilise the properties of qubits and have the potential to outperform traditional computers. The first quantum computing system from IBM was produced in 1998 and had 2 qubits [33]. In 2022, IBM's 433-qubit quantum computer Osprey was introduced [34]. Quantum computing capability allows an increase in the speed of problem-solving up to 100 million times faster than traditional computers [35].

In classical information science, the elementary carrier of information are bits that can be in 2 states, either 0 or 1. A 1-bit classical computer can be (or store/process) in 1 state at a time: 0 or 1. A 1-qubit quantum computer can be (or store/process) in 2 states at the same time. That is $2^1$= 2.  A 2-qubit quantum computer can store $2^2$= 4 possible values simultaneously. Following this simple rule in which the number of values that can be stored simultaneously in a quantum computer would be equal to $2^n$ where n is the number of qubits) significant values can be obtained. This emphasises the power of quantum computing [1]. Unlike a bit, a qubit can exist in a superposition of both states [12]. The processors of classical computers use classical bits to perform their operations. Quantum computers use qubits to run multidimensional quantum algorithms.

In order to visualize the performance of a quantum computer in comparison with classical ones, see Table 1 below. This gives an indication of how powerful quantum computers, especially qubits actually are.

Table 1. Qubit Simultaneous Storage Capacity [1]

| **Classical bits** | **Classical storage (bytes)** | **Quantum storage (bits)** | **Quantum storage (bytes)** |
|---|---|---|---|
| 4 | 1 | 16 | 2 |
| 8 | 1 | 256 | 32 |
| 32 | 4 | 4 294 967 296 | 536 870 912 |
| 64 | 8 | 1.84467E+19 | 2.30584E+18 |

Quantum computers are being developed progressively, and this development is driven mainly by commercial interests [22]. While special purpose quantum computing devices may be available in the mid-term, developing a true general-purpose universal quantum computer, applicable to a range of NATO problems, is likely a long way from being commercially available. As mentioned before, large private companies such as Google and IBM have already come up with their ambitious roadmaps for the development of quantum computers [36] [37].

Present quantum processors are composed of tens to hundreds of physical qubits and cannot sustain fault-tolerant quantum computation. These systems are known as noisy intermediate-scale quantum (NISQ) systems, which are aimed at demonstrating the advantages of quantum computing [38]. However, the ultimate aim is to demonstrate quantum supremacy[1] [38], and development of the Fault-Tolerant Quantum Computer (FTQC). This is a type of a cryptographically relevant quantum computer (CRQC). The goal of FTQC is to enable fault-tolerant computing, thereby converting noisy quantum computers to ideal quantum computers by reaching a perfect logical qubit [23]. Currently, research is focused on quantum error correction (QEC), noise reduction, and exploring various qubit technologies. The evolution of quantum computers towards FTQC can be seen in Figure 1.

[1] Superiority of quantum computers over classical computers for some specific task(s), in some strictly technical sense, practically unattainable for classical computers [12].

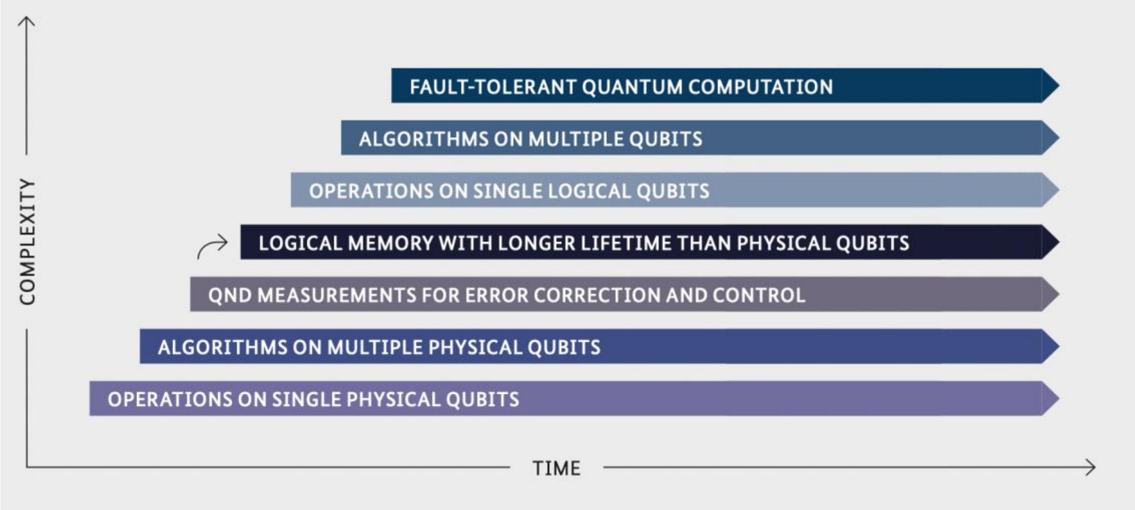

FAULT-TOLERANT QUANTUM COMPUTATION
ALGORITHMS ON MULTIPLE QUBITS
OPERATIONS ON SINGLE LOGICAL QUBITS
LOGICAL MEMORY WITH LONGER LIFETIME THAN PHYSICAL QUBITS
QND MEASUREMENTS FOR ERROR CORRECTION AND CONTROL
ALGORITHMS ON MULTIPLE PHYSICAL QUBITS
OPERATIONS ON SINGLE PHYSICAL QUBITS
COMPLEXITY
TIME

Figure 1. Development Stages for the Construction of a Fault-Tolerant Quantum Computer [39]

A quantum computer of sufficient size and fault tolerance, also known as a Cryptographically Relevant Quantum Computer (CRQC), when available, will be capable of breaking public-key cryptography used on digital systems around the world as well as breaking cryptographic algorithms based on short symmetric keys. It is believed that the quantum threat might rise to prominence faster than we might expect [12]. One field that is expected to be affected by quantum computers is cryptography, i.e. information encryption through algorithms. There is a global race to develop a cryptographically relevant quantum computer (CRQC). Despite the fact that today’s quantum processors are still far from being CRQC, the technology is maturing, so cybersecurity experts should consider it more a matter of “when” than of “if” [12].

When analysing the applicability of quantum computing for military purposes, it is necessary to take into account the technology readiness level (TRL) of what is available on the market and the possibility of reaching the required TRL of QT applicable for NATO. According to the NATO STO, it is not foreseen that a true general-purpose quantum computer, applicable to a wide range of military problems, will be commercially available very soon. According to Kealey and Serna, this can happen no sooner than in 15 to 50 years [40]. However, special purpose devices, e.g., developing new quantum-optimised algorithms and modelling and simulation for defence problems applied to special and limited data or big data and advanced analytics problems, can be made available sooner [22]. In combination with machine learning, quantum computing will allow the processing of higher data volumes. Therefore, as a result, the detection and response of cyberattacks will become more sophisticated [41].

In general, quantum computers, especially when turning the FTQC stage, are believed to have the potential to help scientists and engineers address hard problems that classical computers are not able to solve or are not able to solve quickly enough [25]. These are, e.g., conducting simulations to advance medicine, engineering, mission planning, logistics management, supply chain optimization, energy management optimization, predictive maintenance, medical advancements and material sciences. These represent only a few examples of quantum computer' applications. IBM has set 3 main applications of quantum computers which they could confer. These are simulation, algebraic problems and search [24].

### 2.1.3 Quantum Computing in Cybersecurity

The most obvious application of quantum computing mentioned in the literature is the application of Shor's and Grover's algorithms. According to the German Federal Office for Information Security (BSI), these two algorithms constitute the basis of the quantum threat [42]. The quantum threat is expected to have a huge disruptive impact on the current digitally dependent economy [43]. But not only in the economy but also in another fields, such as the military. Many experts have forecasted that the quantum threat will materialize in 10 years [43]. Due to the secrecy of certain nations looking for strategic advantage, it is most likely to happen sooner than expected [43]. The timeline of quantum threat can be seen in Figure 2 below.

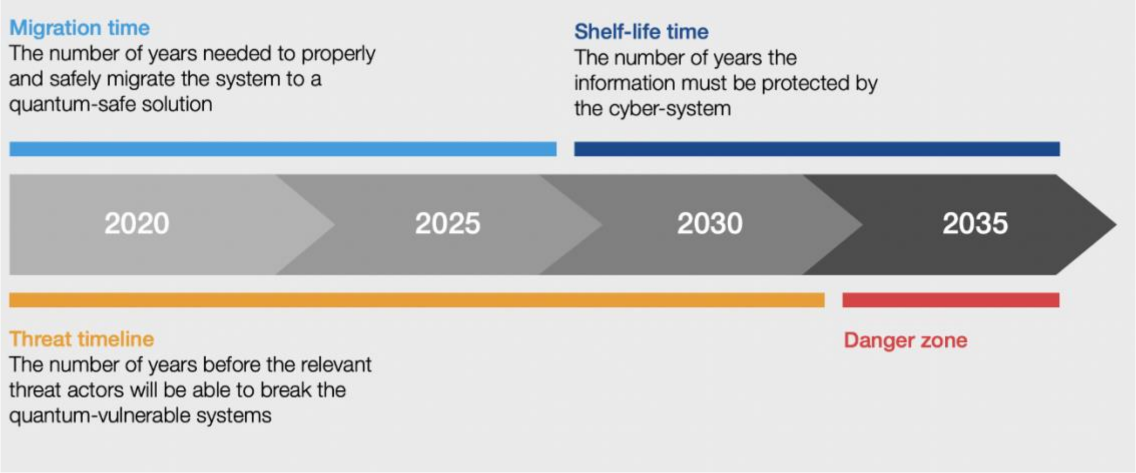

Migration time
The number of years needed to properly and safely migrate the system to a quantum-safe solution
Shelf-life time
The number of years the information must be protected by the cyber-system
2020
2025
2030
2035
Threat timeline
The number of years before the relevant threat actors will be able to break the quantum-vulnerable systems
Danger zone

Figure 2. Quantum Threat Timeline [43]

Quantum computing poses a threat to cryptographic systems that underpin our current methods of cybersecurity. It can break existing public-key encryption standards such as RSA (Rivest-Shamir-Adleman), Diffie-Hellman, ECC or ElGamal cryptosystem [12]. In 1994, mathematician Peter Shor introduced what is nowadays known as Shor's algorithm [44]. This algorithm represents one of the starkest examples of theoretical quantum advantage [45]. Since then, the possibility that quantum computers could be used to break commonly used cryptographic systems has loomed. Breaking current cryptographic methods allows unauthorised decryption, including decryption of all exchanged private or classified messages. Grover’s algorithm will speed up a brute-force search for the key [46]. Therefore, it is also often referred to as quantum “search” [23].

The main focus of the literature talking about the impact of QT on cybersecurity is quantum threat. There’re not many mature literature sources saying about the opportunities of QT for cybersecurity. However, the lines of research in this area currently assume that the emerging field of quantum machine learning may enable more time- and energy-efficient and exponentially faster machine learning algorithms [22]. So, it was found that there is a transformative impact of machine learning on cybersecurity, providing advanced detection and prevention of novel attacks [47].

### 2.1.4 Quantum Communication

NATO's cybersecurity posture is very much reliant on secure and robust communication. This is particularly important in military operations where it is a critical factor in achieving information dominance [48]. Quantum communication promises the exchange of information via an ultra-secure communication network that forms the basis of the so-called quantum internet [49]. Quantum communication is fully based on the quantum phenomena. Quantum phenomena does not send any signals, but it uses entangled quantum particles to send information. To exchange information, the quantum internet uses free-space channels or optical fibre [2]. Quantum internet is believed to allow unhackable networks and transmission of information faster than the speed of light, although in practice, there are still some security vulnerabilities [50] [51]. Quantum communication makes it possible to provide information theoretic security of data transmission [52] [53]. Real-world demonstrations of significant terrestrial and space-based systems have already shown development in this and promise of highly secure global communications [22] [54]. The primary near-term application of quantum communications would be to improve the security of communications against interception and eavesdropping, which is driven by the intelligence community [22] [55].

### 2.1.5 Quantum Key Distribution (QKD)

The first application of the quantum communication principles and the first stage of the quantum internet is a method known as quantum key distribution (QKD). The theory of QKD was established by Charles Bennet and Gilles Brassard in 1984, creating a QKD protocol called BB84 [56].

QKD is a technology that secures the distribution of symmetric encryption keys by relying on quantum physics [57]. QKD uses optical links, to send photons which are "quantum particles" of light. According to the principles of quantum physics, the observation of a quantum state causes perturbation. It means that if someone wants to eavesdrop on the transmitted photons, the transmission will be perturbed. Various QKD protocols are designed in a way that the perturbation leads to transmission errors, and thus, these can be detected by legitimate users. It can be concluded that, QKD implementation therefore requires interactions between legitimate users. And since these interactions need to be authenticated, it can be said, that QKD can use an authenticated communication channel and transform it into a confidential communication channel [57].

QKD end devices are already developed by various industries in the world, for example iDQ and Toshiba [58] [59] [60]. According to the researchers from the Technical

University of Delft, QKD is the first stage of building quantum networks [61]. In the terrestrial applications the distance of the QKD communication is limited to about 100km for fibre-optic links [62]. In order to extend the distance trusted nodes need to be added. Their role is to route keys between distant parties.

QKD provides the opportunity to exchange encryption keys only known between shared parties [63]. The main practical implementation of QKD is to provide the key exchange mechanism for point-to-point encryption between two high-importance endpoints. For the exchange of cryptographic keys, QKD uses quantum channels [50]. After the encryption key is exchanged, the actual data is transmitted over a traditional communication channel [64].

Many security agencies are currently sceptical about using QKD, and they think that it is not yet sufficiently mature from a security perspective, yet as a primary solution to quantum threat [65]. For example, in 2020, The American National Security Agency issued the following statement: "NSA does not recommend the usage of quantum key distribution and quantum cryptography for securing the transmission of data in National Security Systems" [66]. Several security agencies (ANSSI, BSI, NLNCSA, Swedish Armed Forces) in their Position Paper claim that there are particular drawbacks and limitations to successfully implementing it [65].

The Position Paper lists a number of QKD technical limitations [65]. At present, end-to-end security cannot be achieved over fibre-based QKD and long distances, so trusted nodes or repeaters must be introduced. QKD also requires a classical previously authenticated channel between the communicating parties. Also, QKD protocols are subject to a number of different attacks, for example attacks on the protocol [42]. Due to QKD's limitations, it can only be used in some niche use cases.

The application of QKD devices for NATO in a military context must be subject to a certification process by a certification authority. This requires verification of security – security proof, evaluation of attack and threat landscape. There are activities in various standardization bodies, but this work is still in its infancy. In addition, QKD protocols are not yet standardized [42].

There are several QKD devices that are already operational. They are not fully mature in terms of quality, speed and security, but they are functional. In terms of quantum communication, an initiative The Europe Quantum Communication Infrastructure (EuroQCI) was launched in 2019 [67]. By integrating quantum-based systems into existing communication infrastructures, and providing an additional security layer based on quantum physics this project will help to safeguard sensitive data and critical infrastructures. Also, this project reinforces Europe's governmental institutions and it is believed to be one of the main pillars of the EU's Cybersecurity Strategy [68]. Within this project both terrestrial and space segments are being built. For the space segment, the Commission is working with the European Space Agency (ESA) [67]. In cooperation between ESA, the European Commission and space companies in Europe, the first space-based QKD system Eagle-1 will be launched in the fourth quarter of 2024 [69] [70]. European Telecommunications Standards Institute (ETSI) is also working on standardizing QKD interfaces under their standardization initiative ISG-QKD [71] [72].

### 2.1.6 Quantum Information Science

All the areas mentioned above are part of a broader suite of challenges under the general banner of Quantum Information Science (QIS) [22]. QIS includes the research and development (R&D) of quantum computers, algorithms, cryptography, programming languages, modelling, simulation, and knowledge applications. QIS generally explores how information can be encoded in a quantum system, including the associated statistics, limitations, and unique affordances of quantum mechanics [23]. Although QIS is still very immature, considered as a potentially game changing technology for future military operational environment [73].  It is believed to be game changing because it will impact the military operations in the future by bringing new capabilities that were beyond the scope of present technology. It means improving precision and effectiveness of current technology and methods and precision in current measurement technology [2]. It is necessary to provide solutions that can lead from scientific breakthroughs to tangible, game-changing practical applications that can support The Alliance's Warfare Development Agenda (WDA), especially in scope of the following WDIs (Warfare Development Imperatives): Cognitive Superiority, Layered Resilience and Influence and Power Projection, Cross-Domain Command and Integrated Multi-Domain Defence [74] [75]. Investing in QIS can lead the Alliance to gain quantum superiority and outperform adversaries in a technological development in many different areas, for example in diverse military domains [73].

Michael Hayduk, chief of the computing and communications division at the Air Force Research Laboratory, said in 2018 that QT will be “disruptive” in areas such as data security and GPS-denied navigation [76]. The U.S. Air Force is particularly focused on QIS, which is the application of the laws of quantum mechanics to information science.

The transformative power of QIS is still limited due to the infancy of today's quantum hardware [43]. There is a gap in the number of algorithms, as well as software for quantum computer; interfaces, control mechanisms, maintenance, security measures, error correction etc. are necessary. This is why investments in QIS are crucial – those who invests here earlier will faster move forward with the development of robust and mature quantum computers with prospective applications.

## 2.2 Influence of QT on NATO's Cybersecurity

Quantum technologies have a range of potential cybersecurity applications affecting the digital ecosystem. The profound and game-changing impact of quantum computing on cybersecurity can be considered both an opportunity and threat. Quantum technologies, particularly quantum computers, have the potential to pose a threat to existing cryptographic systems and, consequently, to the security of data and communications. There are several potential risks associated with quantum technologies. It is important to note that not all cryptographic protocols are equally affected by quantum computers. It is essential to understand, what are the opportunities and threats of QT to NATO and how NATO can become quantum-ready Alliance as it is stated in NATO's Quantum Strategy [9]. Quantum-ready means that the Alliance is ready to defend against anticipated quantum threats to defence and security, as well as investigate how to proactively leverage the technology [77].

### 2.2.1 Quantum as an Opportunity

Advances in quantum technologies will drastically change the world in the future [78]. They are expected to impact various sectors. One of the examples for the Alliance and military sector would be modelling and simulation, especially in relation to support in decision making and war gaming, as well as solving optimisation problems. But there are many others, especially those that will benefit the Alliance’s security and defence posture.

It is believed that quantum computing will have a profound impact on existing cybersecurity. Quantum computers and technologies, while used by the Alliance, have the potential to drive innovations in diverse military applications, especially in cybersecurity. As outlined before, large-scale quantum computers will expand the current computing capabilities significantly. Thus, quantum computers create new opportunities for improving and bolstering NATO’s cybersecurity. One of the examples is detecting and deflecting quantum-era cyberattacks, before they can cause harm [79]. Quantum technologies, bring the ability to speed up the machine learning, by enhancing its efficacy for cybersecurity. It in turn could expedite the classification of massive amounts of data.

According to the IBM report on quantum technologies, quantum cybersecurity can provide more compelling and robust opportunities to safeguard critical information than currently possible [79]. This is especially important in quantum random number generation (QRNG) and quantum machine learning (QML). Quantum random number generation is essential for cryptography, because it generates the number that is impossible to guess, making them unlikely to be susceptible to cryptanalysis. Therefore, it provides the highest security level [79]. QML explores how to devise and implement quantum software that could enable machine learning that is faster than that of classical computers [80].

Quantum technologies provide unique capabilities that enable to solve problems of complexity and precision that haven’t been possible before and make networks more secure. Quantum-based cybersecurity tools can offer better security than today’s non-quantum equivalents. For example, Quantinuum’s Quantum Origin platform creates stronger encryption keys that are underpinned by the laws of physics by using the unique behaviour of a quantum computer. With the adoption of this technology today, companies can prevent attackers from exploiting weak encryption keys to access encrypted data and systems [41].

### 2.2.2 Quantum as a Threat

There are many concerns regarding quantum technologies, their development and applications. There are also some ethical concerns related to QT meaning that in the wrong hands it can cause harm.

Regardless of exactly when a CRQC becomes available, adversaries can already use one well-known attack [12]. This is called the “Harvest now, decrypt later” attack, which is the most common threat pertaining to cryptography in a post-quantum world. The threat refers to a proactive approach taken by potential adversaries who compromise systems to collect encrypted data today with the intention of decrypting it in the future when quantum computers are powerful enough to break existing encryption methods. It is a fact that HNDL attacks have been a threat already for 10 years and according to the public information, China is one of the countries that is actively implementing those attacks [81].

### 2.2.3 Towards a Quantum-Resistant Cybersecurity

In April 2024 European Commission released its document "Recommendation on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography" [82]. This paper encourages Member States to develop a strategy for the adoption of Post-Quantum Cryptography.

The advantage of quantum computing brings new opportunities but also risks. The decision-makers are those who have to consider both to make the organizations quantum ready. The urgency of this process varies for each organisation, because it depends on the security needs and risk tolerance of the organisation. Only with enough time can a transition to quantum-safe cryptography be implemented safely [12].

To protect the organisation against quantum threat, it will take years, it won’t happen overnight. Therefore, already in 2021, the US Department of Homeland Security issued a legislation to define and implement plans in order to mitigate quantum threat [83]. The acceleration of the research effort on post-quantum[1] cryptography (PQC) started in 2015.

[1] The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that can withstand attacks against both quantum and classical computers, and can existing communication protocols and networks [89]. The terms "post- quantum" and "quantum-resistant" are being used interchangeably.

One of the first steps was the US National Security Agency's release that anticipated a need to shift to quantum-resistant cryptography in the near future [84]. In 2017, the US National Institute of Standards and Technologies (NIST) started the competition for standardization of post-quantum cryptography algorithms [85].

To mitigate the risk of the quantum threat the recommendation from different papers is to implement in the short-term PQC algorithms, when they are standardized, but also – in the medium and long -term – work on QKD and quantum communication in parallel [50] [42]. It should be emphasized that military applications need recommendations from security bodies for using the algorithms, e.g. CNSA 2.0 from the US National Security Agency. The Commercial National Security Algorithm Suite 2.0 already recommends PQC algorithms for key establishment and signature for National Security Systems (NSS)[1] owners, operators and vendors of the future quantum-resistant (QR) algorithms networks [86].

In classified and secret systems, the recommendations are not publicly available, but the transition must be implemented according to the transition plan. Also, this plan should be coordinated with all member states in order to provide interoperability among Allies.

## 2.3 Global Players in Quantum Technologies

Most industrialized countries invest significant resources for research and development into QT. Many of the world's leading nations in QT have started national strategies or initiatives for their implementation and use. The leaders in overall investment are China and the US, but the UK, Canada, Japan, Australia and the EU are also very important players. Many geopolitical players like China, the US and Russia have already developed their own prototypes of quantum computers [87].

It is clearly seen that China and the US dominate across government spending and private investments and it is well known that China is the main threat actor concerning QT [88]. China's rapid rise in the field can be attributed to their government's prioritisation of high technologies in their strategic planning which includes significant investments in QT,

[1] Networks that contain classified information or are otherwise critical to military and intelligence activities.

such as quantum computing, quantum communication and quantum sensing. China, and to some extent Russia, are making investments and innovation progress in QT. For instance, China is the global leader in public funding of quantum computing [90]. Currently, the US is the world leader in quantum computing and sensing, while China is leading the quantum communication field. And once again to mention here, China is the only country that has successfully launched a satellite capable of transmitting quantum-secure intercontinental communication, albeit at limited amounts [55]. Regarding quantum communication, China is considered to be world leader in this field [55]. According to their reports, they have built a fully operational quantum network that connects more than 30 nodes between Beijing and Shanghai over more than 2000 km [91]. In is clearly seen that there is a shift of the technological burden to Asian countries, which are currently investing enormously in the development of both artificial intelligence and QT. In March 2021, the Chinese government, in its 14th Five-Year Plan listed several technology fields that are considered to be essential to its national security and overall development, including QT. Since 2017 China has invested 10 billion US dollars in a centre for QT, with the aim of getting to hold the record for the world's longest quantum-encrypted communication channel (1203 km). This is a big step towards China's main ambition – to become a technological superpower and a global science and innovation leader by 2050 [92].

Big technology companies like Google, IBM and Microsoft have committed hundreds of millions of dollars to research and development in the area of quantum computing [93] [94] [95] [64]. Similarly, governments have recognised the geopolitical value and transformative potential of QT applications and the US, the EU and China have each set up their own >1 billion dollar research programmes [64]. The Pentagon is concerned that quantum computing is one area that is playing catch-up while China continues to leap ahead [76]. The US government is trying to pass laws that will mandate government agencies to use Post Quantum Cryptography (PQC) algorithms for public keys [96]. Also, the Dutch Security Agency AIVD has recently published the Post Quantum Crypto Migration Handbook that provides guidance on a Post Quantum Cryptography [97].

But not only China is actively working on quantum, also Russia. By the end of this year, Russian experts expect a 50-qubit quantum computer [98]. Russia has already introduced their 16-qubit quantum computer. In 2021, Russian government announced that over the next five years, it would invest $790 million in quantum computing research [98]. Russia has also understood the power of quantum and they have decided to invest in it to develop their technological capabilities and become a leader in the global economy.

Knowing the global players in QT is important for several reasons. First and foremost, the development of QT depends on the security of the supply chain. In order to secure the supply chain, the EU has defined new policies on critical raw materials (CRMs).  In March 2023, the European Commission launched the CRM Act to safeguard the security of supply materials that are essential for future and current technologies [99]. The significance of this regulation was emphasized by the Chinese export control restrictions on CRMs, such as gallium, germanium and graphite as a part of their strategic competition with the US [100]. This kind of activities clearly limit the access of NATO countries to CRMs that are critical for the development of QT.

# 3 Methodology

This chapter describes the methodology that was used to investigate the topic of QT and cybersecurity. The research methodology for this thesis was influenced by "Research Methods for Cybersecurity" [101]. Based on this book it can be said that this thesis is an exploratory study. In exploratory studies the emphasis is on relative importance and perspective. This thesis was written with the aim of gaining insights and understanding by evaluating and analysing the data collected, not creating new designs or models.

The primary research question for this thesis is "How does the development of quantum technologies influence the cybersecurity and security posture of NATO?". Investigating the topic of quantum technologies is based on an examination of the current developments, initiatives, and technological achievements. Sources of this information include government publications and online papers from a wide range of sources, including NATO and other defence organisations. The research utilises both quantitative and qualitative research methods, including observations as well as textual or visual analysis. To collect information for the research, international experts from NATO member states were sent a survey. These were supplemented by some interviews. The feedback from the survey together with various academic publications, was the main input for the final thesis. These provided important factual data and strategic insights. The survey was designed to enable a quantitative assessment of the collected data to be made. The results of this research will be of benefit in designing defence strategies specifically tailored to counter state and non-state adversaries and threat actors.

## 3.1 Research Method

Finding the best research method for this thesis was not an easy task, since the topic is very complex and target group is small. The book mentioned above initially suggests identifying a research path, by determining possible research questions [101]. The research started off with very generic questions, but the book suggested to break research questions down to into as small pieces as possible. By following these recommendations, it was helpful to focus and guide the research.

For this research, qualitative and quantitative research methods were used. This thesis was written by analysing and examining published academic and non-academic papers, but in addition to that the author of the thesis decided also to do survey research. Survey research is believed to have its roots in American and English "social surveys" that were conducted around the turn of the 20th century, where reformers and researchers wanted to document the extent of various social problems, such as poverty [102]. In order to conduct the survey research, a survey based on the Delphi method was created. The survey gave an opportunity to analyse the data qualitatively and quantitatively. Quantitative research included the collection and analysis of numerical data, while qualitative method involved the collection and analysis of descriptive data [101]. This kind of hybrid method was chosen because the author found it the most reliable and trustworthy. The quantitative part of the survey provided a statistical exploration and explanation of data by showing the general views of the experts in numbers and figures. The qualitative part as comments section was like a small interview – the respondents had the opportunity to give more insights and explain their opinion. Though both quantitative and qualitative research approaches possess their own strengths and weaknesses, their combination can prove highly effective [103].

## 3.2 Survey

Regarding the measurement of results, a survey was utilized, wherein participants provided written responses.The survey was designed to enable the results to be assessed both quantitatively and qualitatively. With regards to measuring the results Google Forms was used. The author was aware that the medium through which a survey was conducted impacted the formatting of the questions and possible answers. The book that was mentioned above emphasized to think through very wisely to ensure that the chosen medium provides the best opportunity in collecting the necessary data [101]. Google Forms was chosen as a tool because it was very easy to collect and analyse the data, because it created the charts and graphs of collected data itself. Also, it was very comfortable to share the survey with potential respondents. It was decided to use an online tool, because with the Internet it was easy to reach the highest number of subjects. The responses were kept anonymous, meaning other participants were unaware of who provided each answer.

In this survey, two types of questions were used. To be correct, one was a statement, and the other one was comments section. The first part of the survey, a statement, was a rating scale question [101]. This gave an opportunity to provide a range of valued answers that ranged from low to high. The form of the answer was limited, but it still enabled the respondents to express their opinion. For the purpose of this thesis, Likert's scale was employed for this question. 34 questions were presented using the 5-point Likert scale to enable the data to be analysed. This 5-point Likert's scale consisted of 5 points - (1) Strongly Disagree; (2) Disagree; (3) Neither Agree nor Disagree; (4) Agree; (5) Strongly Agree [104]. Open-ended questions, in the case of this thesis comments section, provided the opportunity to fully express the opinions and views of the participants. Respondents were given the chance to provide comments on the topics addressed in the survey, which were supplemented with a follow up interview with some of the participants. Each respondent retained the option to revise their own answers and add additional comments [105]. So, the mathematical method for data analysis was not possible to use while analysing open-ended questions, but it was used for rating scale questions. The data collected form the survey with the Likert's scale was assessed qualitatively [106]. The data collected from the comments section was analysed qualitatively.

One of the research methods that was used was a variation of the Delphi method, which was developed by the RAND Corporation in the 1950s [107]. The same method was used in the report about the applications of QT which was one of the recourses of the thesis [55]. The aim of this method has been to preserve the benefits of a collaborative group while avoiding potentially detrimental group dynamics, such as the influence of dominant individuals who may not be the most qualified experts. The Delphi method is a systematic approach used for gathering and refining the insights of a group of experts. Traditionally, the Delphi method uses multiple rounds of data collection through a series of surveys, but in this thesis a variation of this method was used, therefore only one round of surveys was conducted. The Delphi method is especially valuable in master's thesis research, when addressing intricate or emerging subjects lacking consensus among experts. The experts' responses remained anonymous, providing them the freedom to express opinions without concern for judgment or external influence. The method's iterative process allows for ongoing refinement and consensus development across multiple rounds. The surveys were carefully structured to guide experts' responses and extract specific information. A Delphi panel should encompass experts with diverse backgrounds, experiences, and perspectives, ensuring a comprehensive range of viewpoints is considered [107]. The Delphi method was also chosen for this research as that it was formulated to forecast the influence of technology on warfare in the early stages of the Cold War [108] and remains applicable today.

## 3.3 Ethical Considerations

Ethical aspects of the thesis were considered while conducting the research. In compliance with ethical research guidelines the participants were informed about the purpose of the study and data collection. Before the respondent started answering the survey, the person showed its consent to be part of the research by ticking the box provided. The respondents were given informed consent about the research, stating the purpose of the study.

The use of survey as a research tool is a risk for biases. According to this research, for example the Hawthorne effect and demand characteristics were considered. The Hawthorne effect is a tendency in people’s behaviour when they know that are being observed [109]. It means that they may have the desire to give different answers, they answer the way they want the author of the research to see their answers. Demand characteristics refers to a behaviour of giving responses that the participants of the research think the research is about [110]. It means that there can be some cues that can influence participants in a certain way so they can distort the genuine responses. The author of the thesis might have been biased due to personal views and opinion, but she could confirm that the survey was not biased, having neither a positive nor negative view. The aim was to create the survey as precise and clear as possible and to make sure that the questions were phrased in a neutral way not using words with ambiguous or vague meanings, so there was no indication that particular answers were preferred or expected. That was the reason why the survey was created in a way that for almost every statement there was a reverse statement, so the respondents could not predict what kind of answer was expected from them. This also gave an opportunity to validate the answers by asking the opinion of about one aspect but in a different way.

Respondents participated in the survey on a voluntary basis, and they had the opportunity to withdraw from the study at any time. The conductor of the research can confirm that the answers to the survey were not manipulated after collecting and none of the responses were removed from the collected data. The data was solely collected for this thesis.

All the respondents answered the survey once as it was seen from the collected data, who had responded. In this research full names and emails were requested to control who participated in this survey and to contact the respondents to ask additional questions if needed. Some people were concerned about their anonymity, since they wanted to represent their personal views and they did not want their views to be linked to the company or institution they were working for. The confirmation about anonymity protected the privacy of the participants and likely contributed to more honest and accurate responses.

The survey used in the Delphi method contained topics from all research questions. The aim of this survey was to find out what are the attitudes among experts from various disciplines related to cybersecurity and QT. The questions were crafted to evaluate participants' perspectives on the application and repercussions of QT in terms of NATO deterrence and defence, specifically regarding cybersecurity. Specifically, these individuals were asked to participate in the survey regardless of age, gender, professional and educational background or nationality. The only condition was that they work with QT on a daily basis, either in private or public sector. The target group comprised representatives of NATO Headquarters, NATO Communications and Information Agency (NCIA), Air Force Research Laboratory (AFRL), The Netherlands Organisation for Applied Scientific Research (TNO), Karlsruhe Institute of Technology, Deloitte, Thales Group and many more. The author wants to highlight the fact that some of the people who responded to the survey were also authors of some referenced publications in this thesis. Therefore, the quality of the research done for this thesis is at a high level. Some people who were contacted did not want to participate in the research, because they did not feel comfortable answering the survey, since they did not consider themselves to be experts in quantum field.

The primary ethical concern of the survey could potentially be the presence of biased questions. Even though it was endeavoured to maintain neutrality in the questions, the problem of politically motivated decisions and opinions persisted. Since NATO is a political and military Alliance, expert opinions may not be based on science but on politics. It had been tried to avoid and mitigate it by involving experts from different nationalities, both from the public and private sectors. It was emphasized in the beginning of the research that the data collected from the survey was anonymous, meaning that no specific answers were connected to a person. The views and opinions were only presented in a general way. Regarding the Likert's scale, each participant might had ultimately interpreted the provided options on the Likert scale in a distinct manner, since the author did not have a direct contact with the target audience. The study did not encounter any ethical concerns.

## 3.4 Limitations

The target audience's language was confined to the English-speaking community. Also, one of the limitations for this research was the fact that all the respondents had to be from NATO member states.

## 3.5 Validation of Methods

In order to validate the chosen research method, in this case, the results of the survey, some non-structured expert interviews were conducted. The interviews were held verbally with some of the respondents who provided answers that stood out from the crowd. There were held 4 interviews. One of the interviews that was part of the research was also published in NATO’s Technology and magazine NITECH [111]. Also, one more interview will be published in the same magazine in July 2024.

# 4 Results

This chapter presents the data obtained by collecting responses from quantum experts to a survey. The survey was sent to the participants via email, some of the experts were also contacted via LinkedIn. The results were collected during the period of March 20th until April 5th, 2024. The response rate was 31,6%, meaning that out of 76 surveys sent, 24 responses were received.  It is accepted that this response rate is low, and a higher number of replies would have been preferable. Although the author knew that it was hard to get answers to the survey according to the complexity of the topic and the difficulty to contact experts from quantum field. Since this was not a broad internet survey that everyone could answer, the sample itself was already very small and the number of the respondents was already expected to be rather small as well. However, expertise of the people that responded corresponds with high quality of responses. The survey consisted of 34 statements that the respondents had to evaluate according to the Likert scale from 1 as Strongly disagree to 5 as Strongly Agree. Not every responded gave their comments to all questions, but all respondents assessed all the statements provided. The survey is replicated in Appendix 2.

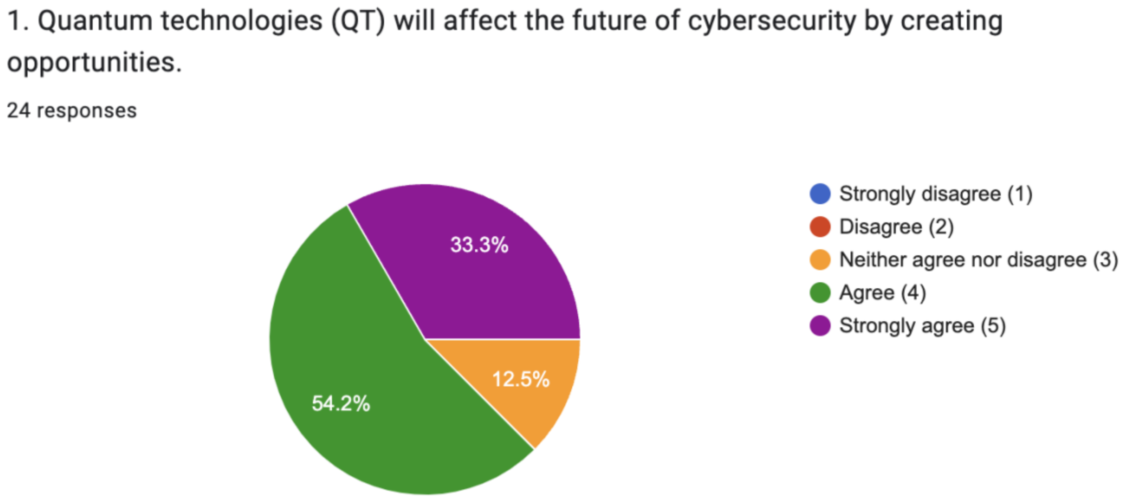
Before starting to evaluate the statements, the participants had to write their name, current employer and current job position. The list of participants regarding the employer and job position can be seen in the Table 2 below.

Table 2. Overview of the Participants by Current Employer and Job Position

| Current employer | Number of people | Current job position |
|---|---|---|
| NATO Communications and Information Agency (NCIA) | 7 | Senior Scientist (2), Senior Cybersecurity Specialist (3), Chief Service and Technology Strategy, Project Manager (Innovation) |
| NATO Headquarters | 2 | Digital Transformation Architect, Deputy Head of NATO Innovation Unit |
| The Netherlands Organisation for Applied Scientific Research (TNO) | 3 | Head of Business Development Electromagnetics & Military Operations (also NATO STO Chair for QT Coordination |

| | | |
|---|---|---|
| | | Committee), Professor, Quantum Scientist |
| Fox Crypto NL | 1 | Security Architect |
| Deloitte | 1 | Quantum Cyber Readiness Leader |
| Thales Group | 1 | Quantum Algorithms & Computing Segment Leader |
| NATO Science and Technology Organisation - Centre for Maritime Research and Experimentation (STO-CMRE) | 1 | Scientist |
| Air Force Research Laboratory (AFRL) | 1 | Physicist |
| Diehl Defence | 1 | Head of Competence Center for EO/EM Systems |
| Fraunhofer IOSB | 1 | Group Leader |
| Deimos Engenharia | 1 | Account Manager for Defence |
| Czech Technical University in Prague / RHEA Group | 1 | Researcher/ Quantum Security Expert |
| Karlsruhe Institute of Technology | 1 | Research Assistant |
| Niels Bohr Institute, Quantum Deep Tech Lab | 1 | Business Developer |
| QuTech | 1 | Quantum Internet Division Engineering Lead |

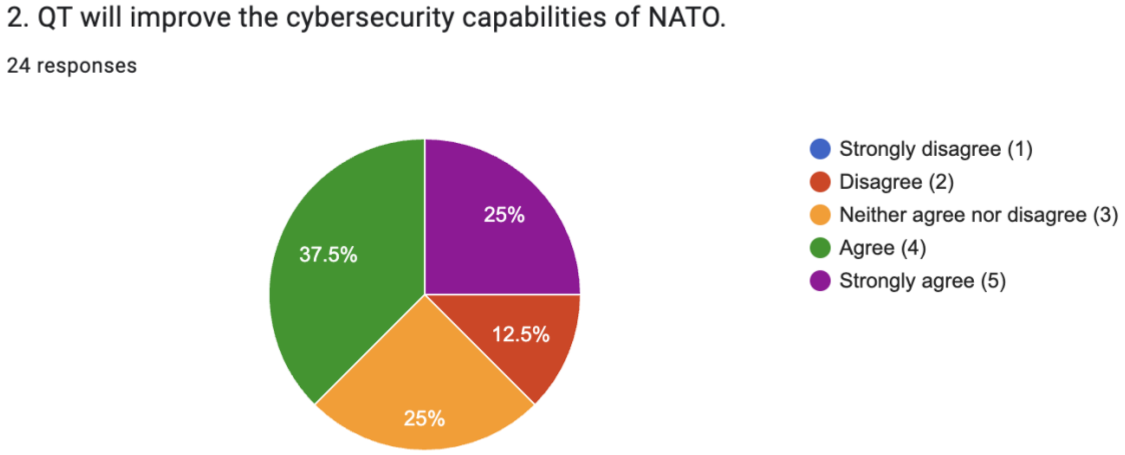
After participants provided their information, they were able to start evaluating the statements. The data collected can be seen below.



1. Quantum technologies (QT) will affect the future of cybersecurity by creating opportunities.

24 responses

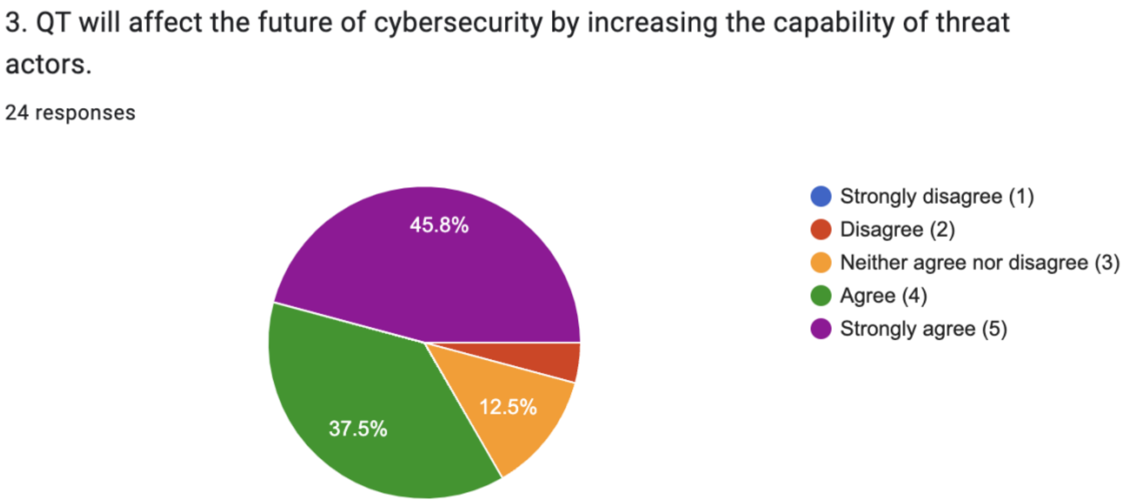
Figure 3. Responses to Statement 1



2. QT will improve the cybersecurity capabilities of NATO.

24 responses

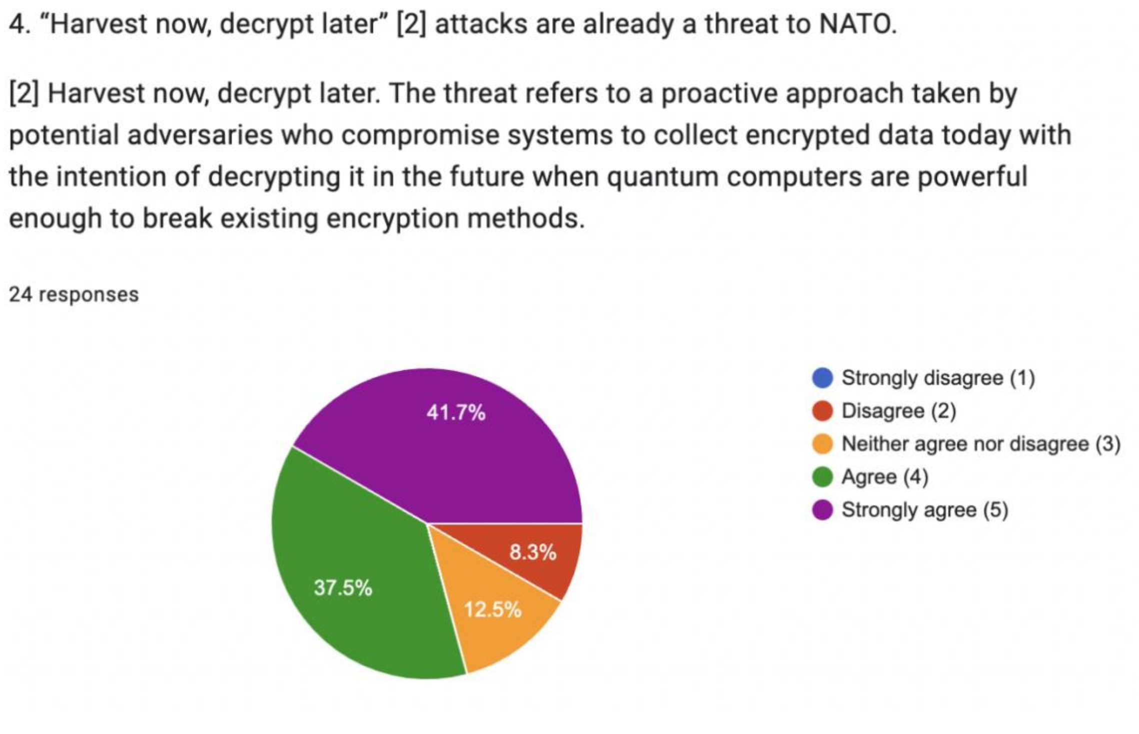
Figure 4. Responses to Statement 2



3. QT will affect the future of cybersecurity by increasing the capability of threat actors.

24 responses

Figure 5. Responses to Statement 3

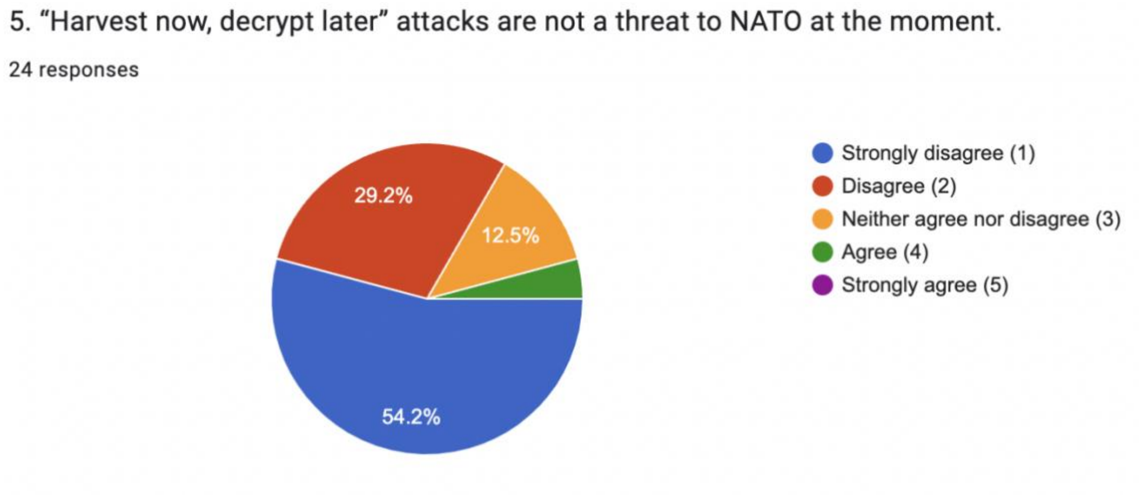


4. “Harvest now, decrypt later” [2] attacks are already a threat to NATO.

[2] Harvest now, decrypt later. The threat refers to a proactive approach taken by potential adversaries who compromise systems to collect encrypted data today with the intention of decrypting it in the future when quantum computers are powerful enough to break existing encryption methods.

24 responses

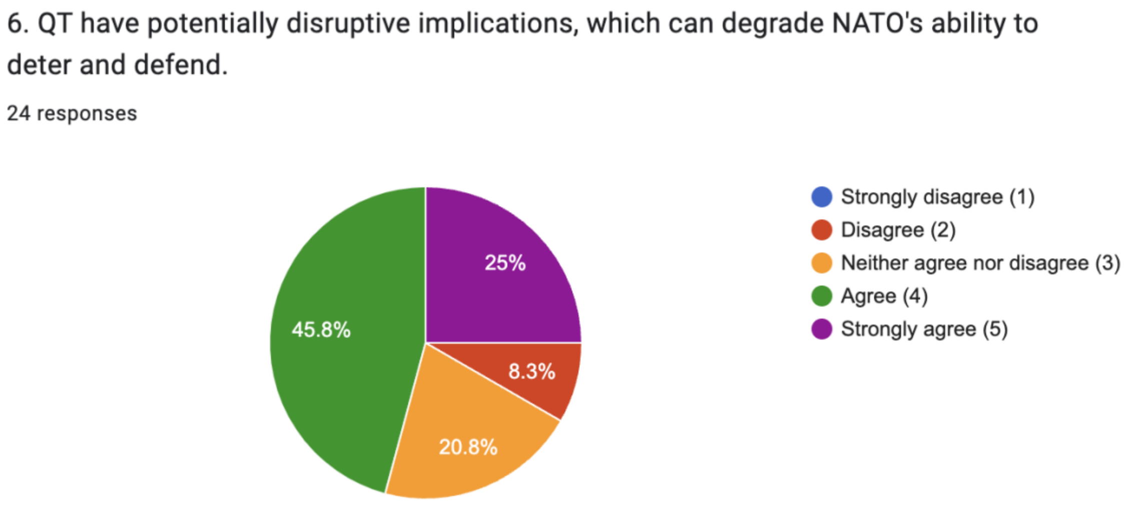
Figure 6. Responses to Statement 4



5. “Harvest now, decrypt later” attacks are not a threat to NATO at the moment.

24 responses

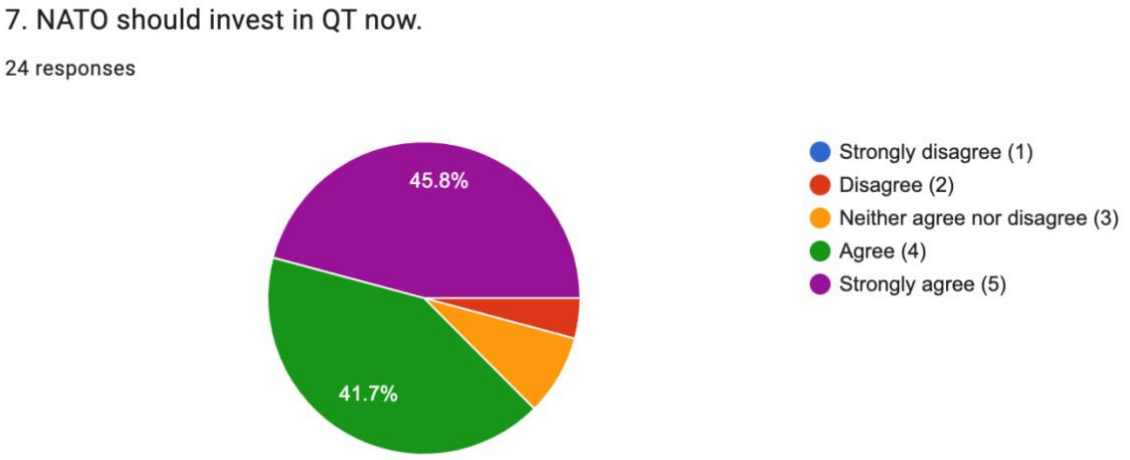
Figure 7. Responses to Statement 5



6. QT have potentially disruptive implications, which can degrade NATO's ability to deter and defend.

24 responses

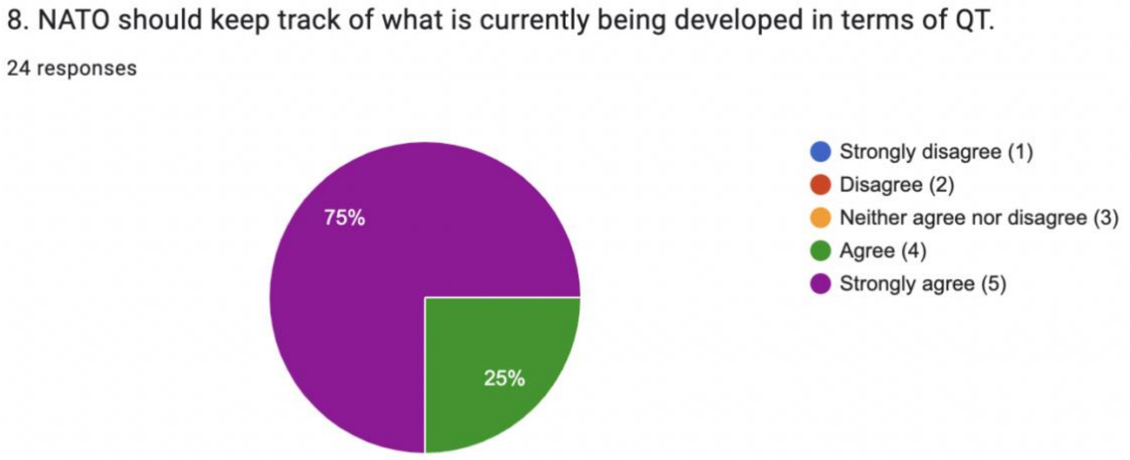
Figure 8. Responses to Statement 6



7. NATO should invest in QT now.

24 responses

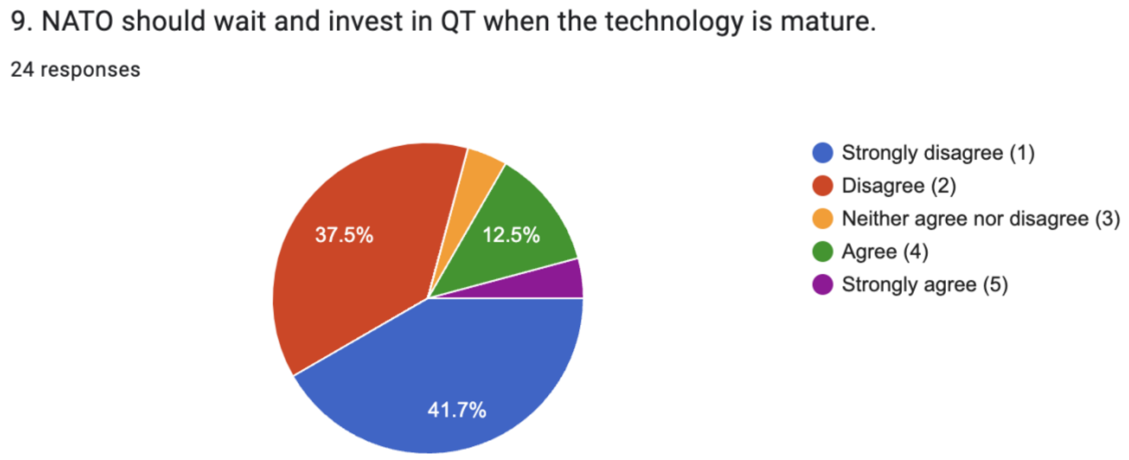
Figure 9. Responses to Statement 7



8. NATO should keep track of what is currently being developed in terms of QT.

24 responses

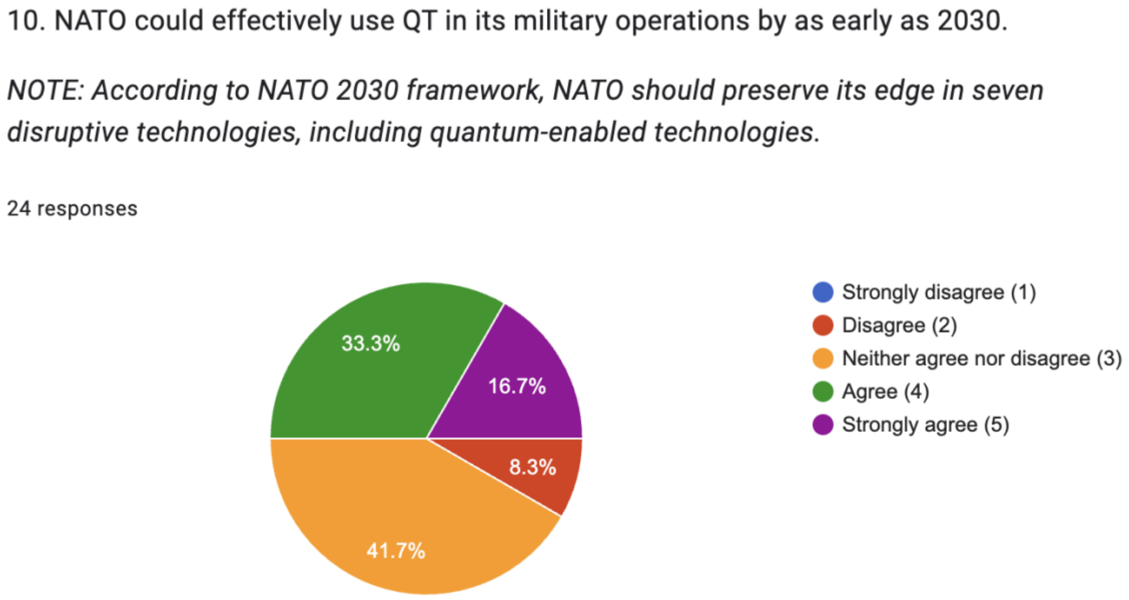
Figure 10. Responses to Statement 8



9. NATO should wait and invest in QT when the technology is mature.

24 responses

Figure 11. Responses to Statement 9

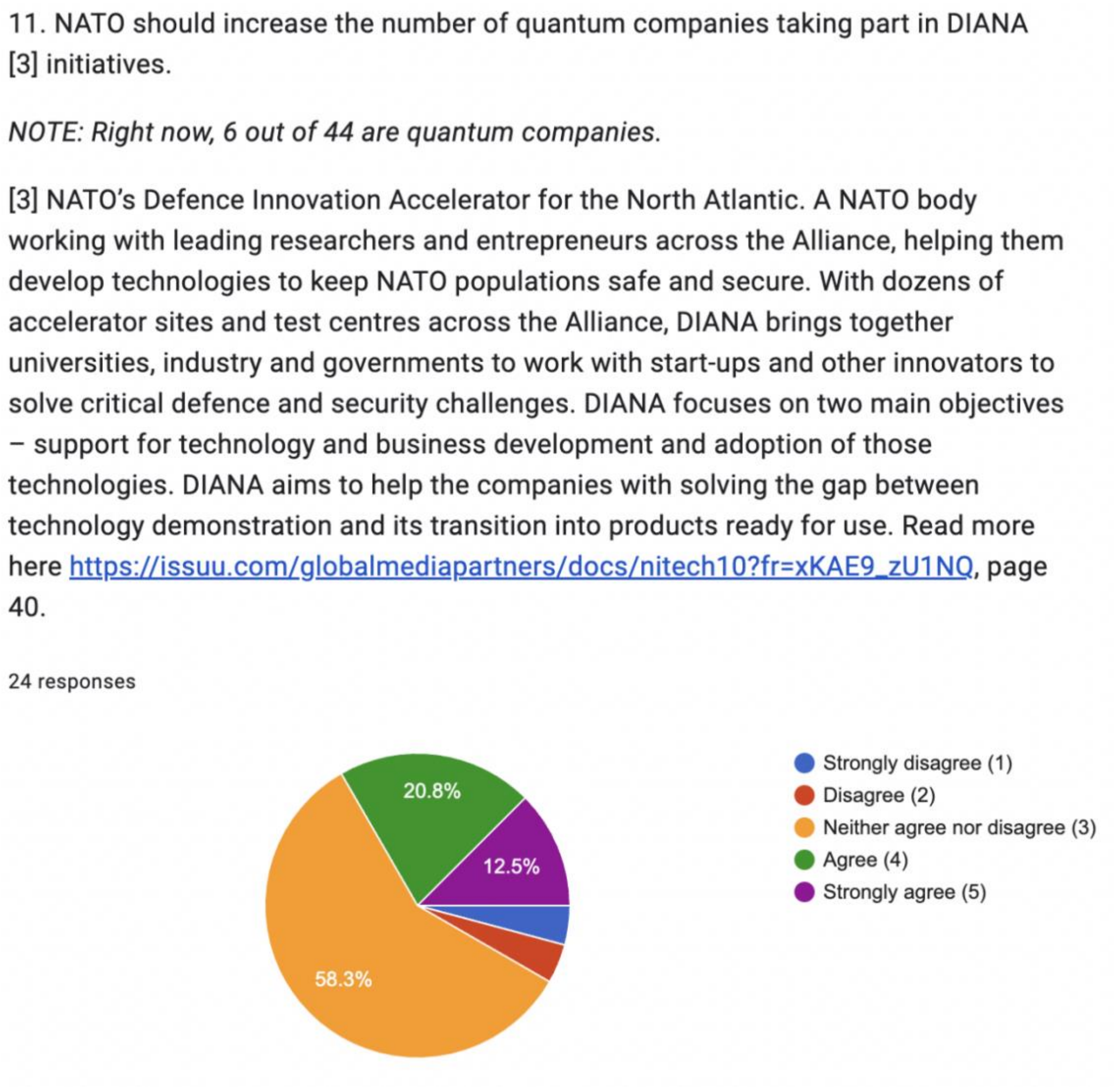


10. NATO could effectively use QT in its military operations by as early as 2030.

*NOTE: According to NATO 2030 framework, NATO should preserve its edge in seven disruptive technologies, including quantum-enabled technologies.*

24 responses

Figure 12. Responses to Statement 10



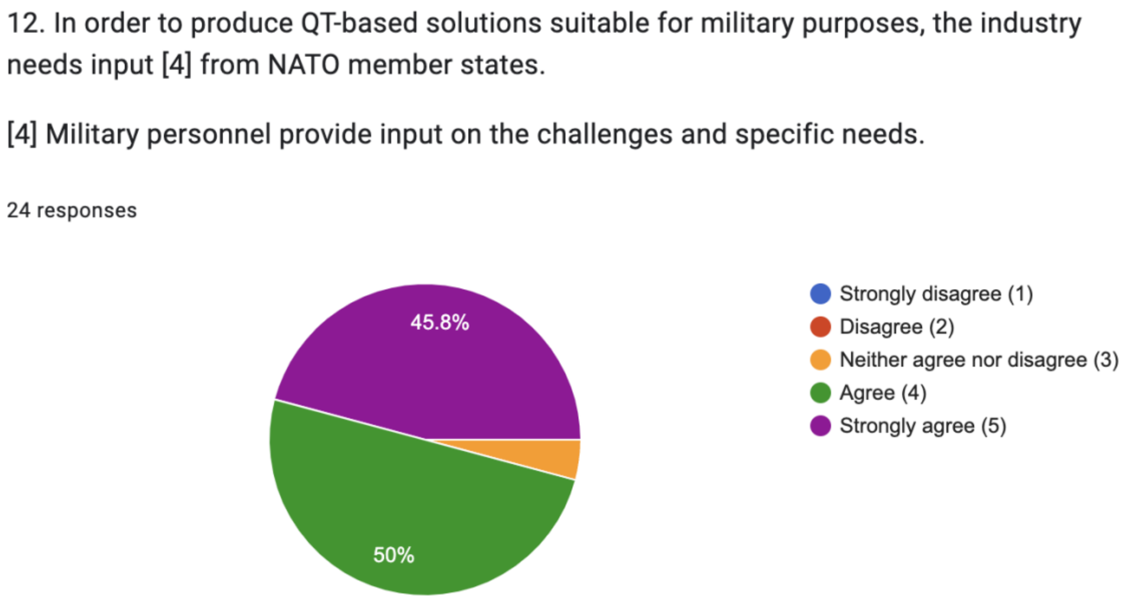
11. NATO should increase the number of quantum companies taking part in DIANA [3] initiatives.

*NOTE: Right now, 6 out of 44 are quantum companies.*

[3] NATO's Defence Innovation Accelerator for the North Atlantic. A NATO body working with leading researchers and entrepreneurs across the Alliance, helping them develop technologies to keep NATO populations safe and secure. With dozens of accelerator sites and test centres across the Alliance, DIANA brings together universities, industry and governments to work with start-ups and other innovators to solve critical defence and security challenges. DIANA focuses on two main objectives – support for technology and business development and adoption of those technologies. DIANA aims to help the companies with solving the gap between technology demonstration and its transition into products ready for use. Read more here https://issuu.com/globalmediapartners/docs/nitech10?fr=xKAE9_zU1NQ, page 40.

24 responses

Figure 13. Responses to Statement 11

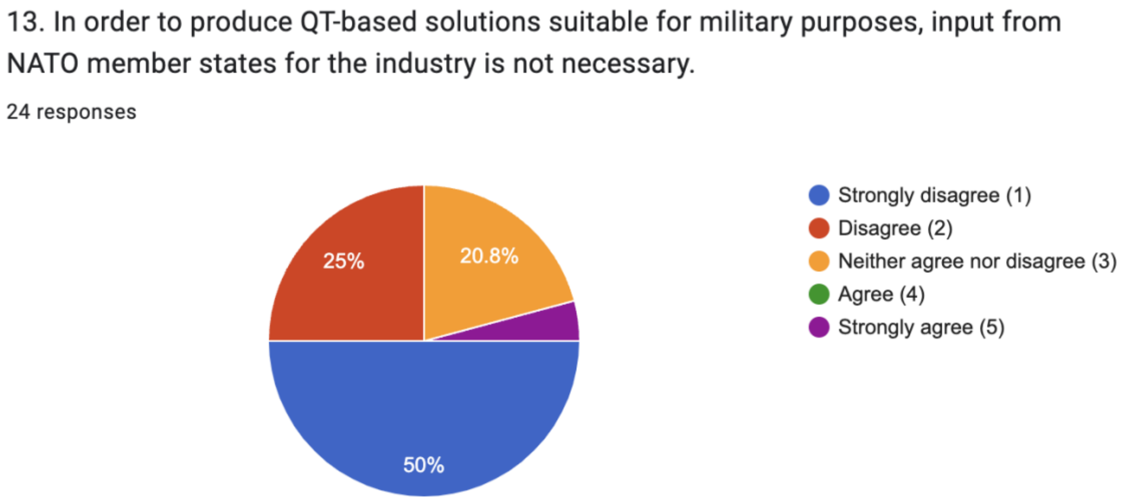


12. In order to produce QT-based solutions suitable for military purposes, the industry needs input [4] from NATO member states.

[4] Military personnel provide input on the challenges and specific needs.

24 responses

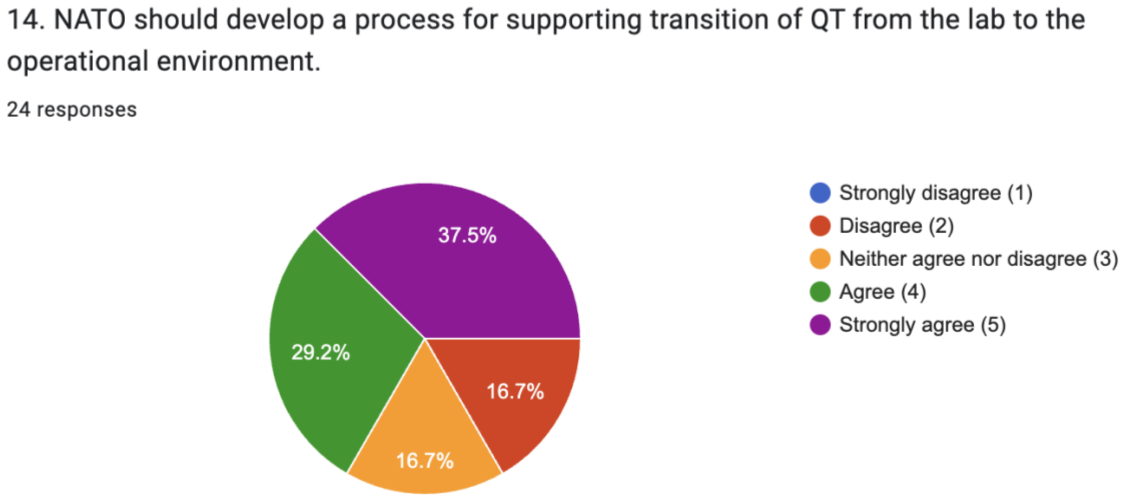
Figure 14. Responses to Statement 12



13. In order to produce QT-based solutions suitable for military purposes, input from NATO member states for the industry is not necessary.

24 responses

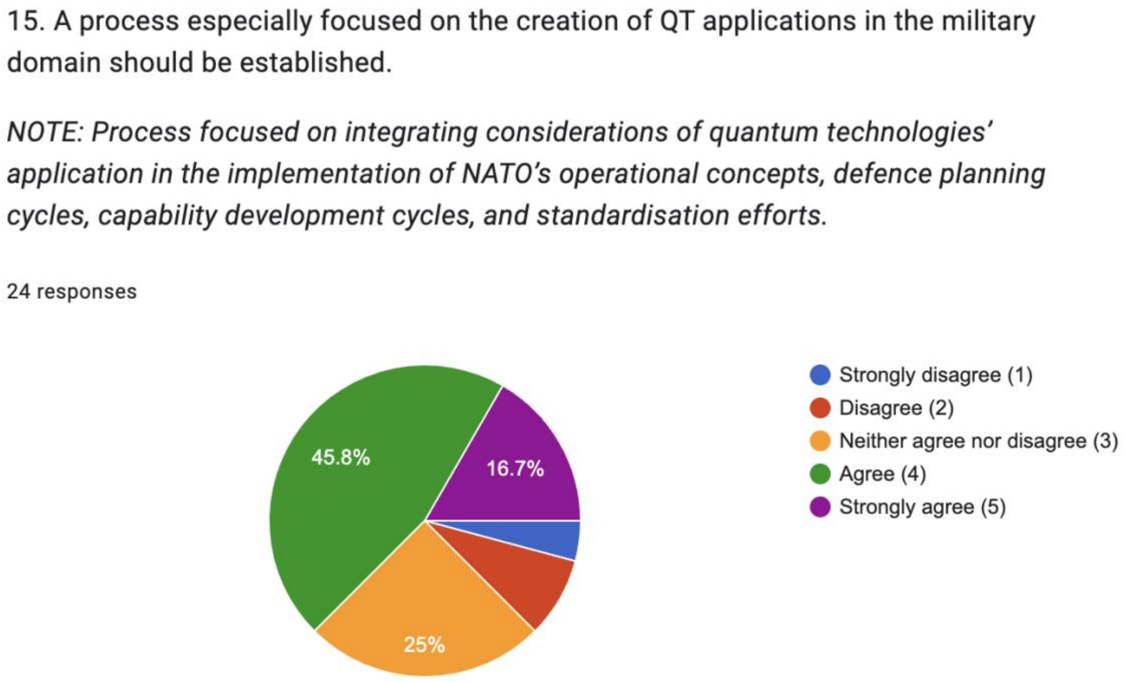
Figure 15. Responses to Statement 13



14. NATO should develop a process for supporting transition of QT from the lab to the operational environment.

24 responses

Figure 16. Responses to Statement 14

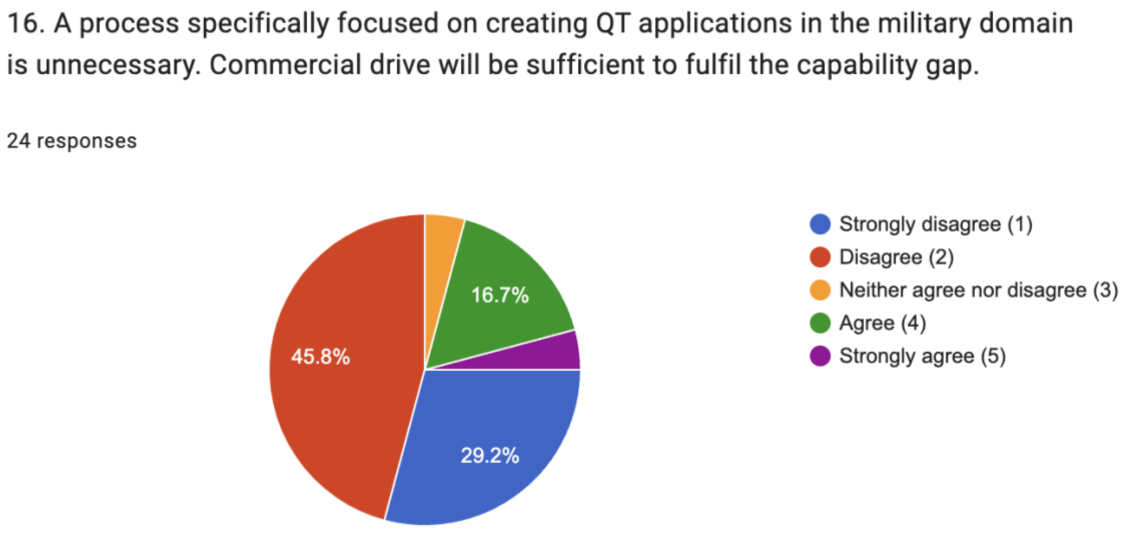


15. A process especially focused on the creation of QT applications in the military domain should be established.

*NOTE: Process focused on integrating considerations of quantum technologies' application in the implementation of NATO's operational concepts, defence planning cycles, capability development cycles, and standardisation efforts.*

24 responses

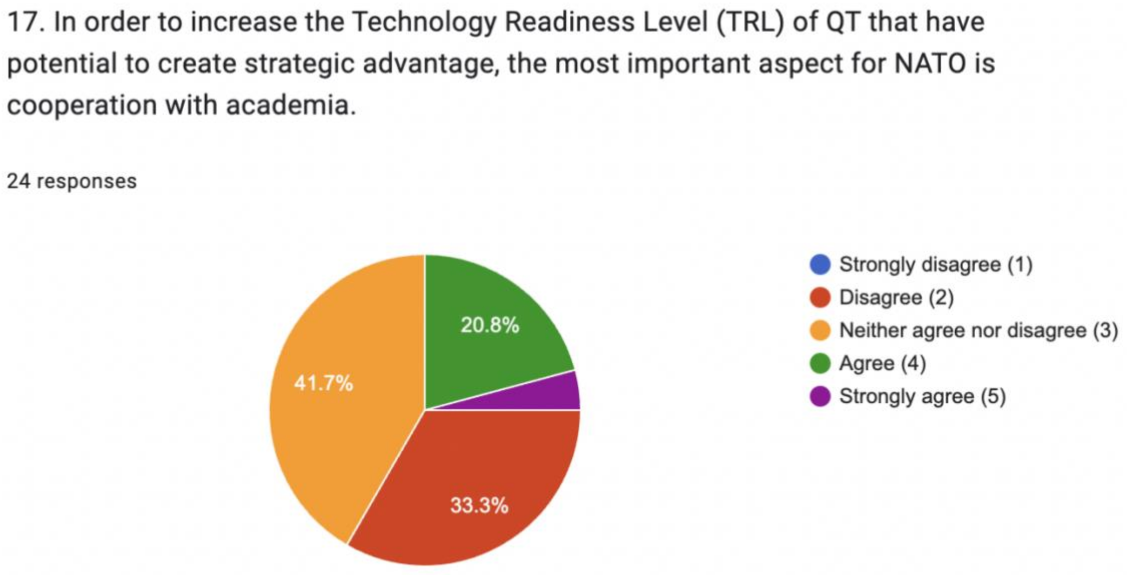
Figure 17. Responses to Statement 15



16. A process specifically focused on creating QT applications in the military domain is unnecessary. Commercial drive will be sufficient to fulfil the capability gap.

24 responses

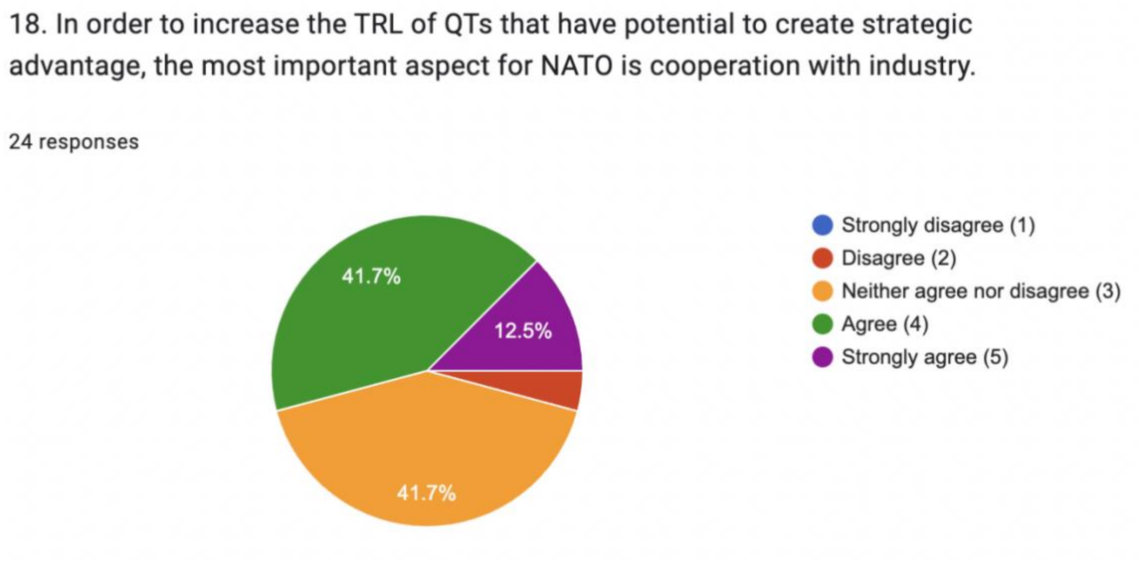
Figure 18. Responses to Statement 16



17. In order to increase the Technology Readiness Level (TRL) of QT that have potential to create strategic advantage, the most important aspect for NATO is cooperation with academia.

24 responses

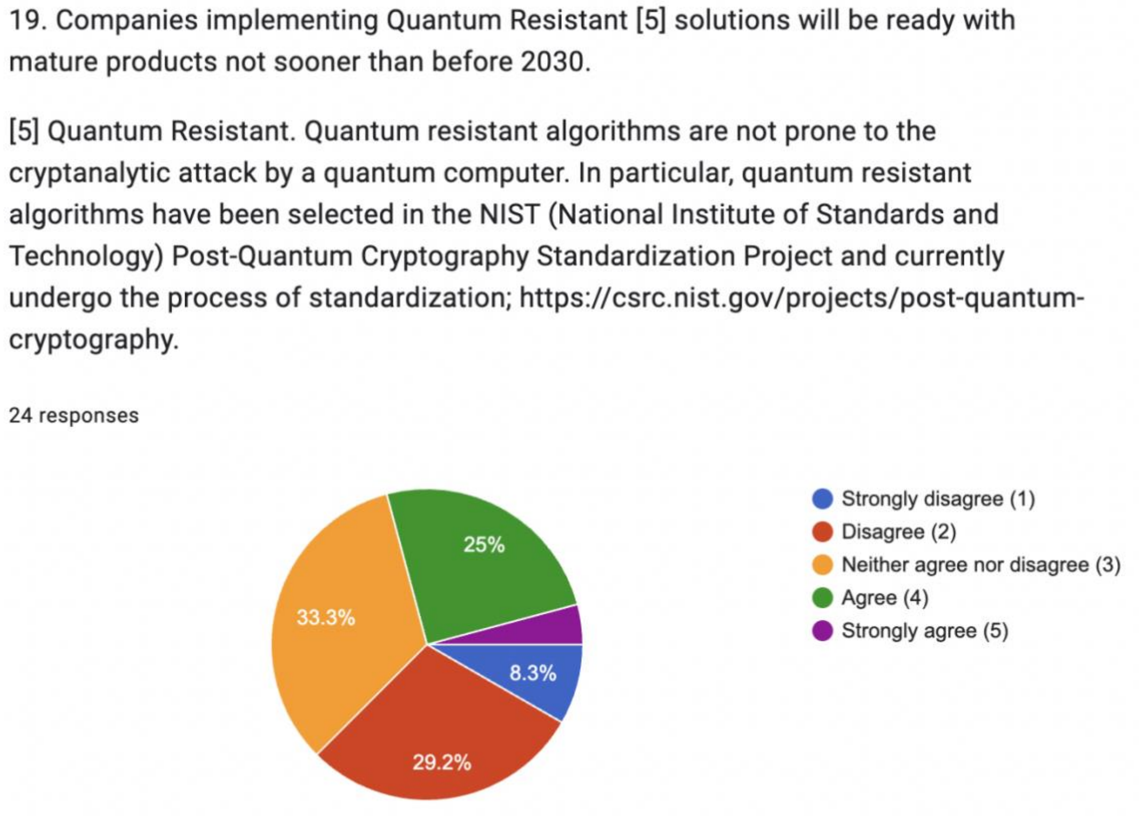
Figure 19. Responses to Statement 17



18. In order to increase the TRL of QTs that have potential to create strategic advantage, the most important aspect for NATO is cooperation with industry.

24 responses

Figure 20. Responses to Statement 18

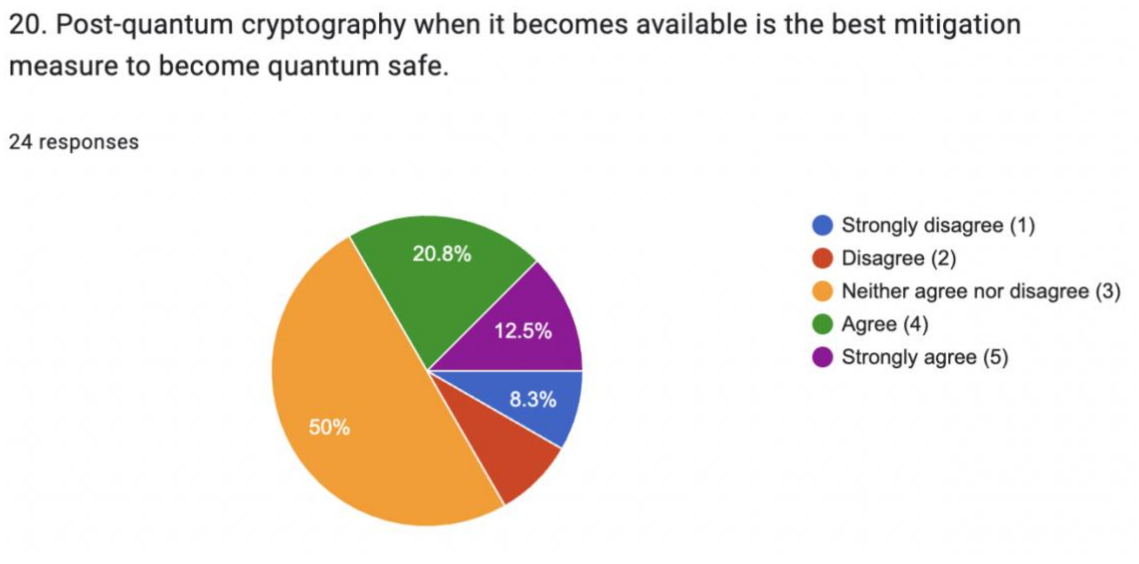


19. Companies implementing Quantum Resistant [5] solutions will be ready with mature products not sooner than before 2030.

[5] Quantum Resistant. Quantum resistant algorithms are not prone to the cryptanalytic attack by a quantum computer. In particular, quantum resistant algorithms have been selected in the NIST (National Institute of Standards and Technology) Post-Quantum Cryptography Standardization Project and currently undergo the process of standardization; https://csrc.nist.gov/projects/post-quantum-cryptography.

24 responses

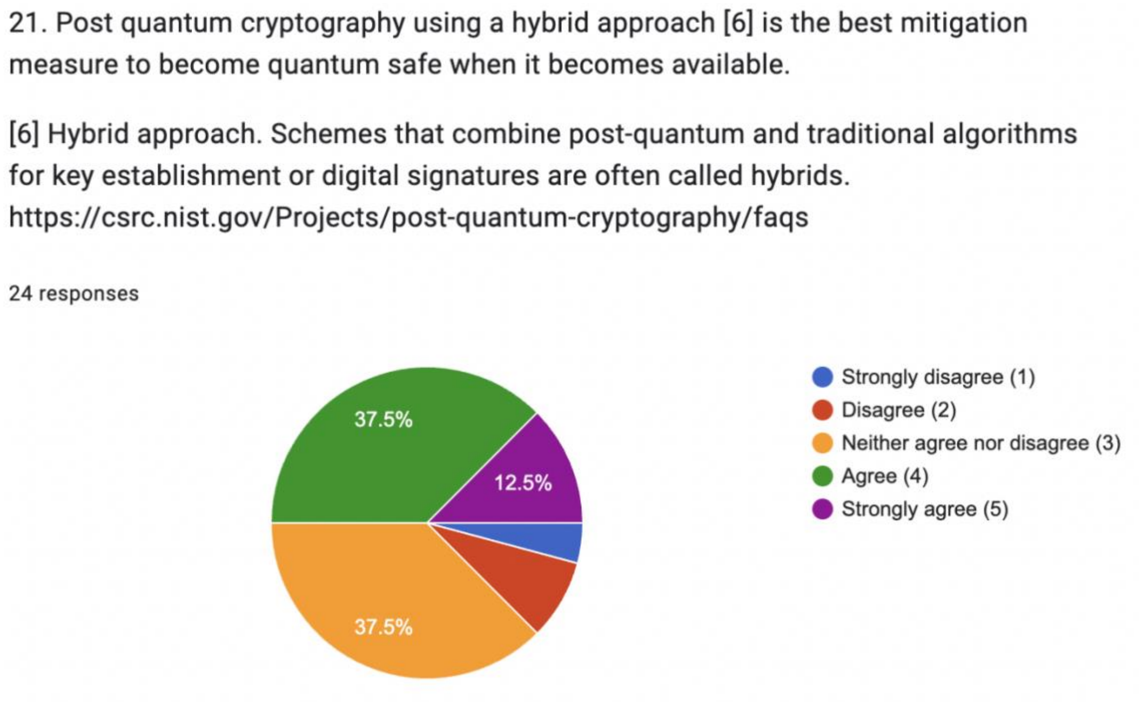
Figure 21. Responses to Statement 19



20. Post-quantum cryptography when it becomes available is the best mitigation measure to become quantum safe.

24 responses

Figure 22. Responses to Statement 20

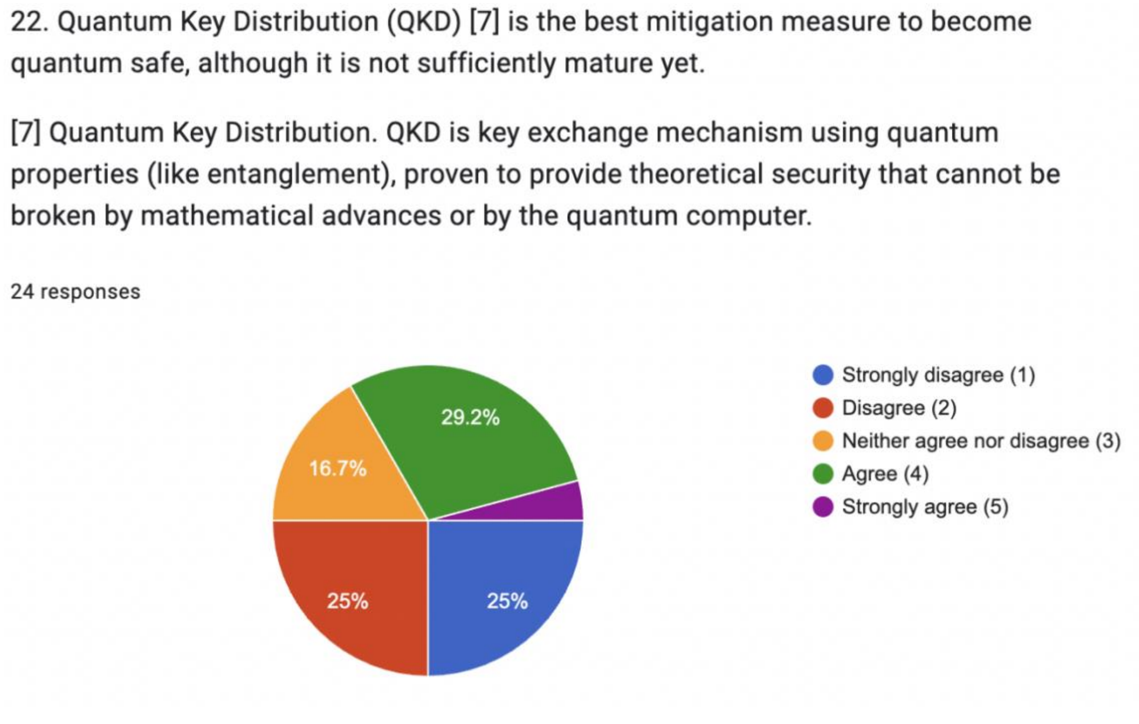


21. Post quantum cryptography using a hybrid approach [6] is the best mitigation measure to become quantum safe when it becomes available.

[6] Hybrid approach. Schemes that combine post-quantum and traditional algorithms for key establishment or digital signatures are often called hybrids. https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs

24 responses

Figure 23. Responses to Statement 21

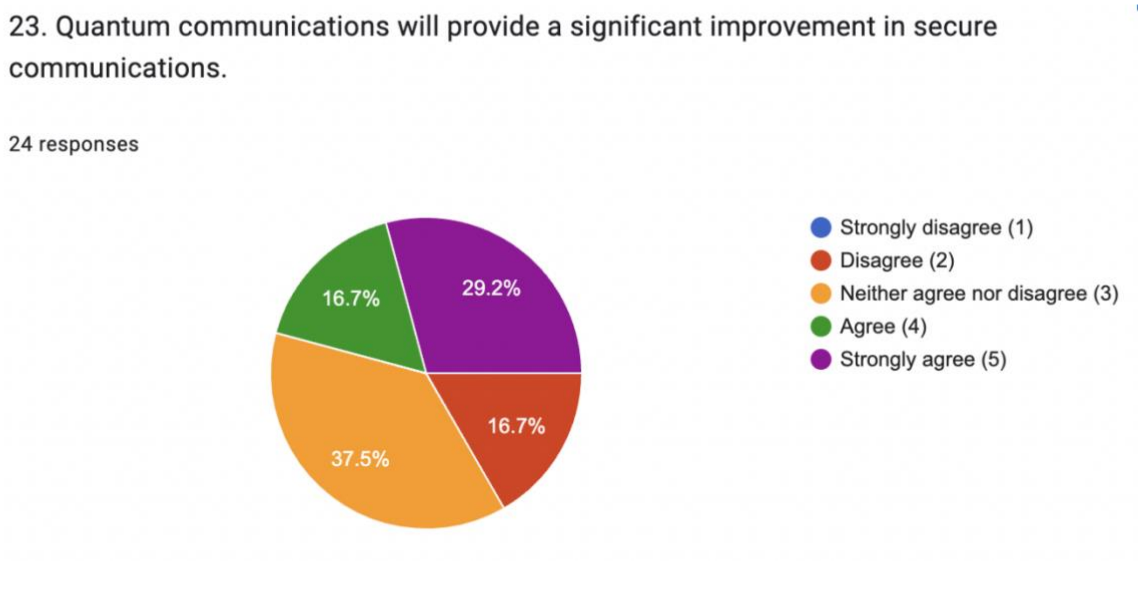


22. Quantum Key Distribution (QKD) [7] is the best mitigation measure to become quantum safe, although it is not sufficiently mature yet.

[7] Quantum Key Distribution. QKD is key exchange mechanism using quantum properties (like entanglement), proven to provide theoretical security that cannot be broken by mathematical advances or by the quantum computer.

24 responses

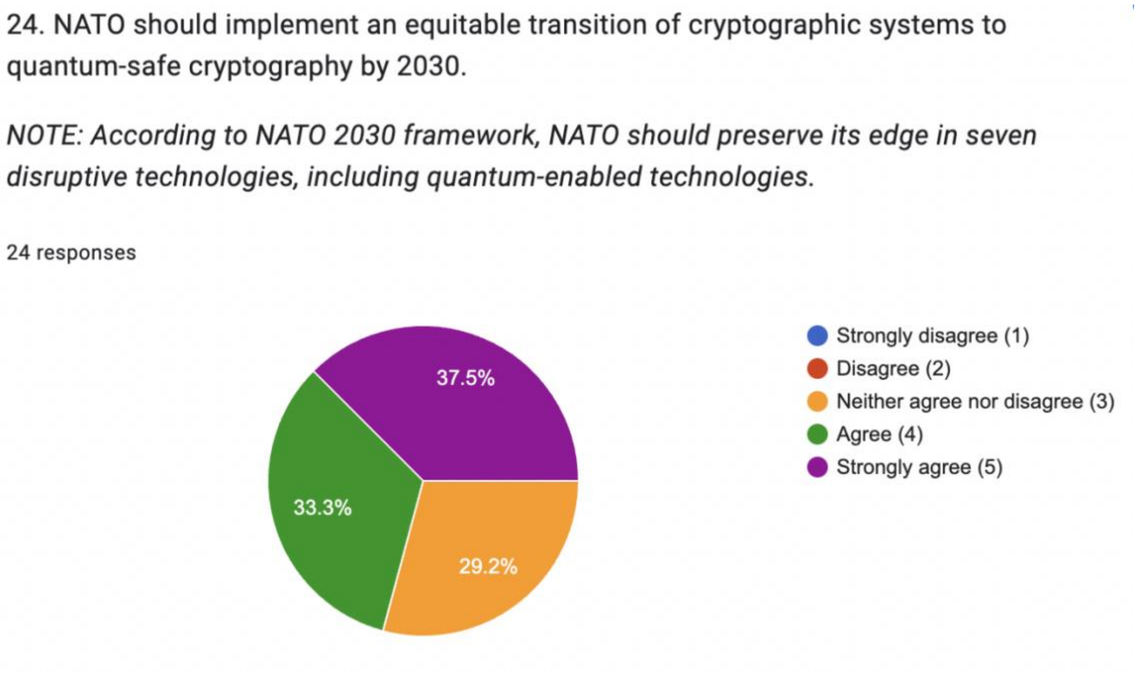
Figure 24. Responses to Statement 22



23. Quantum communications will provide a significant improvement in secure communications.

24 responses

Figure 25. Responses to Statement 23

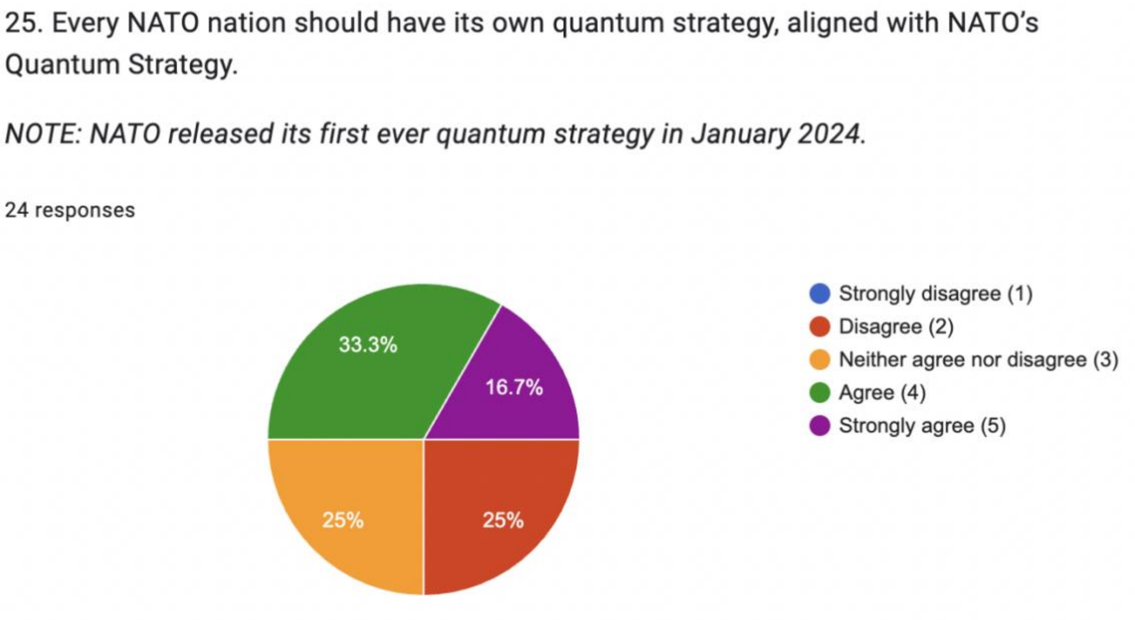


24. NATO should implement an equitable transition of cryptographic systems to quantum-safe cryptography by 2030.

*NOTE: According to NATO 2030 framework, NATO should preserve its edge in seven disruptive technologies, including quantum-enabled technologies.*

24 responses

Figure 26. Responses to Statement 24

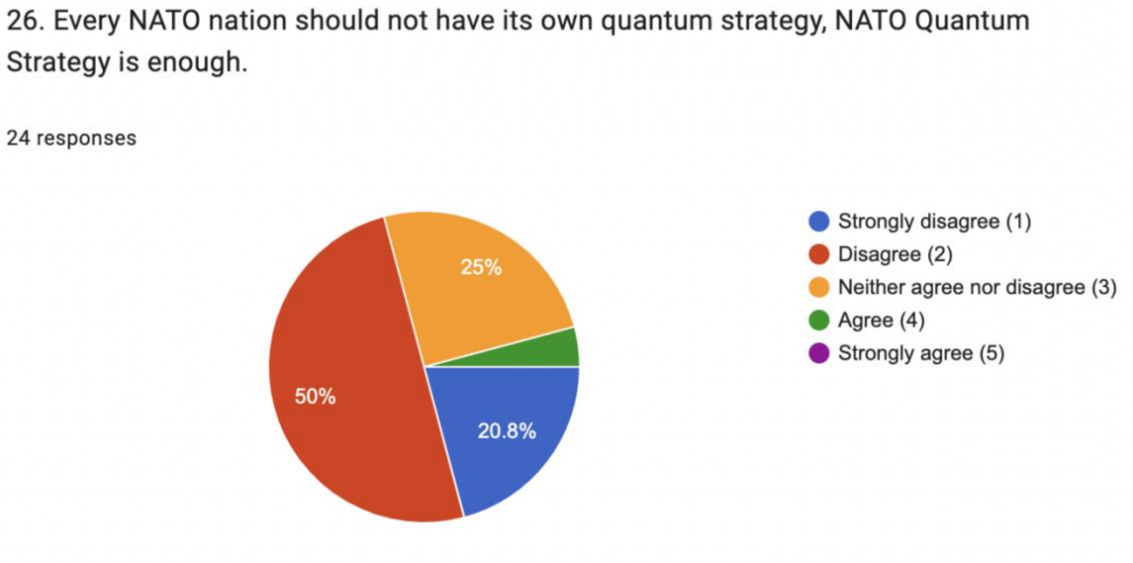


25. Every NATO nation should have its own quantum strategy, aligned with NATO's Quantum Strategy.

*NOTE: NATO released its first ever quantum strategy in January 2024.*

24 responses

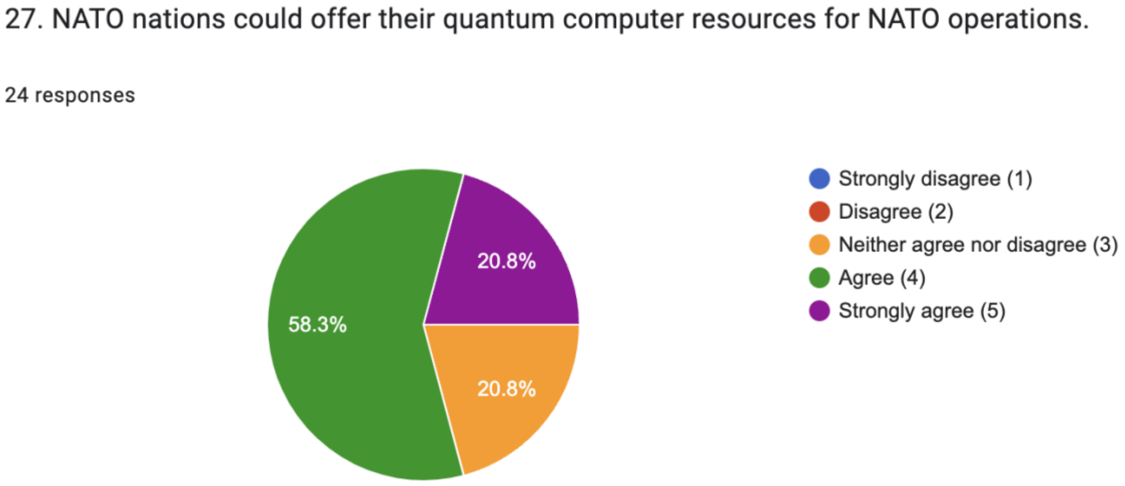
Figure 27. Responses to Statement 25



26. Every NATO nation should not have its own quantum strategy, NATO Quantum Strategy is enough.

24 responses

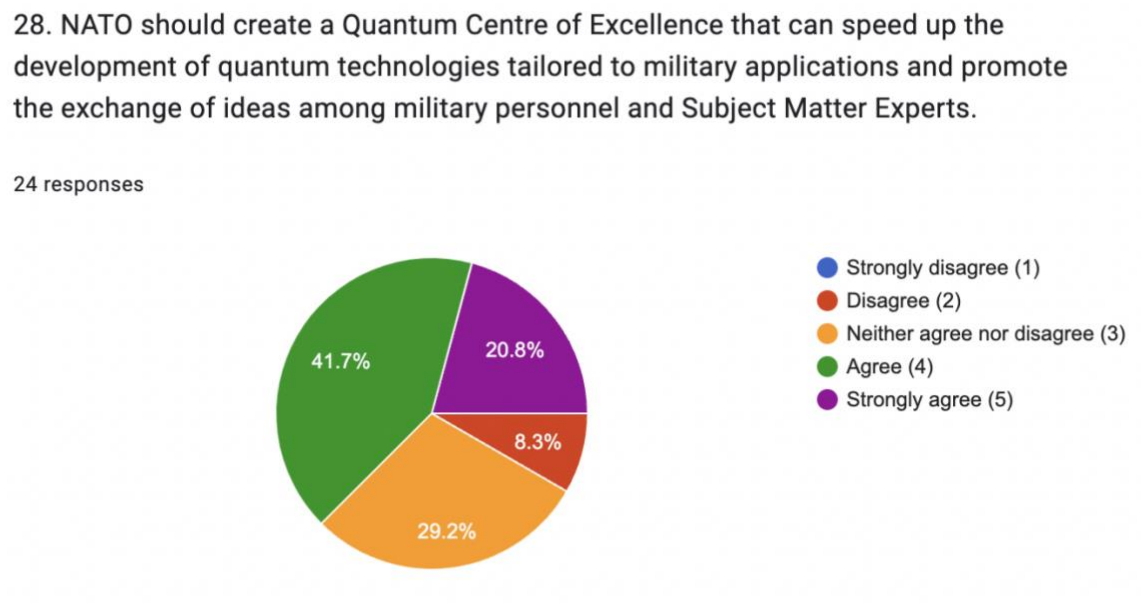
Figure 28. Responses to Statement 26



27. NATO nations could offer their quantum computer resources for NATO operations.

24 responses

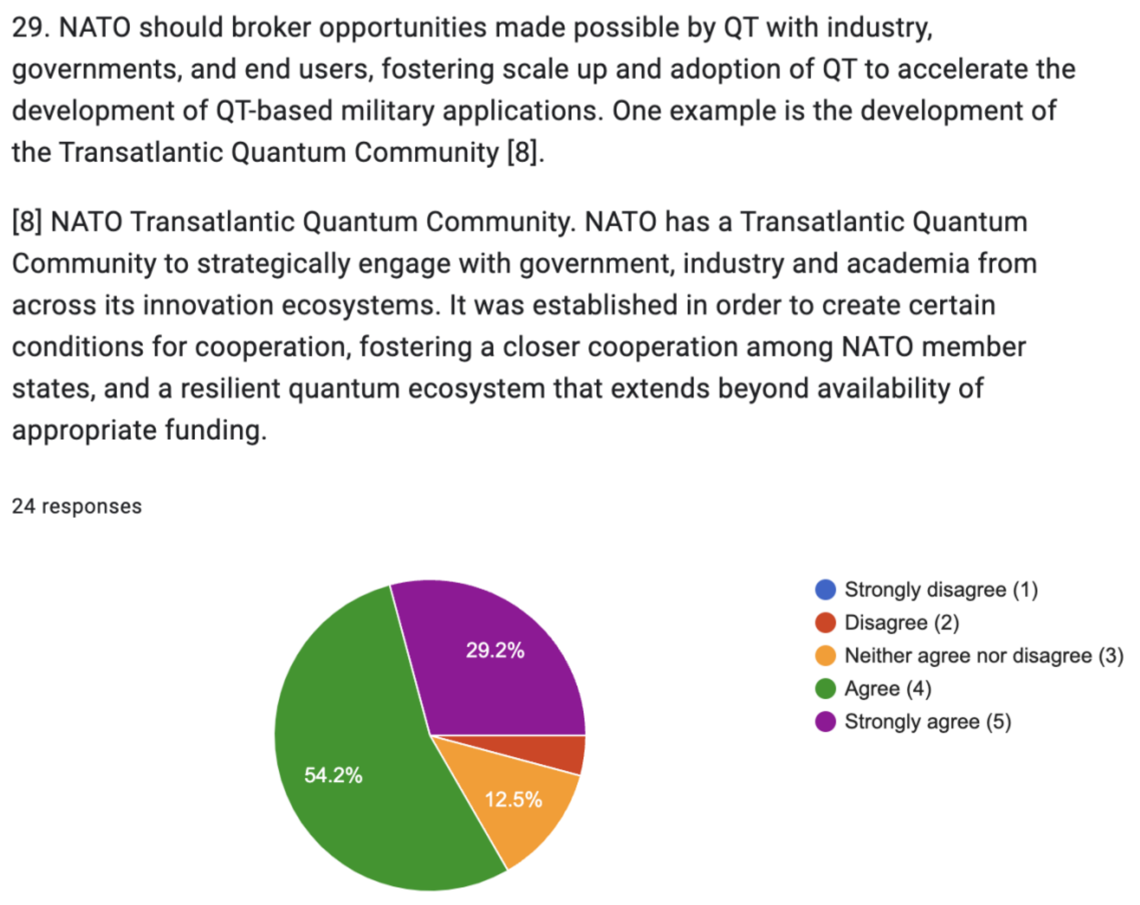
Figure 29. Responses to Statement 27



28. NATO should create a Quantum Centre of Excellence that can speed up the development of quantum technologies tailored to military applications and promote the exchange of ideas among military personnel and Subject Matter Experts.

24 responses

Figure 30. Responses to Statement 28

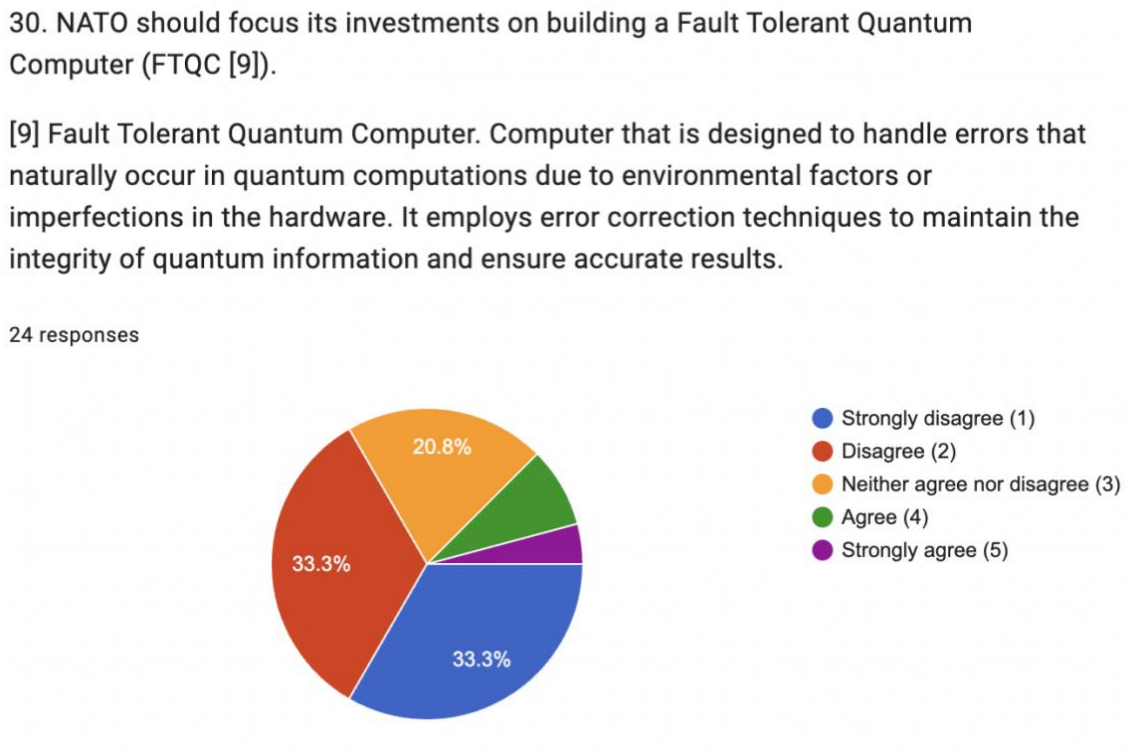


29. NATO should broker opportunities made possible by QT with industry, governments, and end users, fostering scale up and adoption of QT to accelerate the development of QT-based military applications. One example is the development of the Transatlantic Quantum Community [8].

[8] NATO Transatlantic Quantum Community. NATO has a Transatlantic Quantum Community to strategically engage with government, industry and academia from across its innovation ecosystems. It was established in order to create certain conditions for cooperation, fostering a closer cooperation among NATO member states, and a resilient quantum ecosystem that extends beyond availability of appropriate funding.

24 responses

Figure 31. Responses to Statement 29

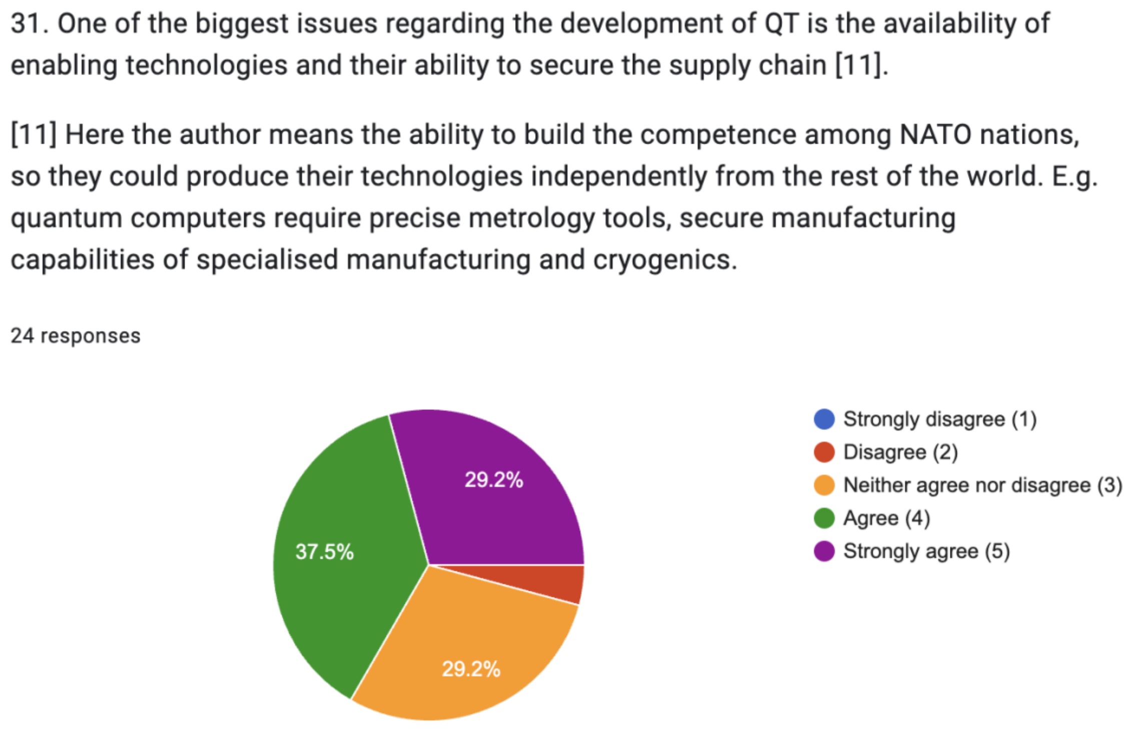


30. NATO should focus its investments on building a Fault Tolerant Quantum Computer (FTQC [9]).

[9] Fault Tolerant Quantum Computer. Computer that is designed to handle errors that naturally occur in quantum computations due to environmental factors or imperfections in the hardware. It employs error correction techniques to maintain the integrity of quantum information and ensure accurate results.

24 responses

Figure 32. Responses to Statement 30

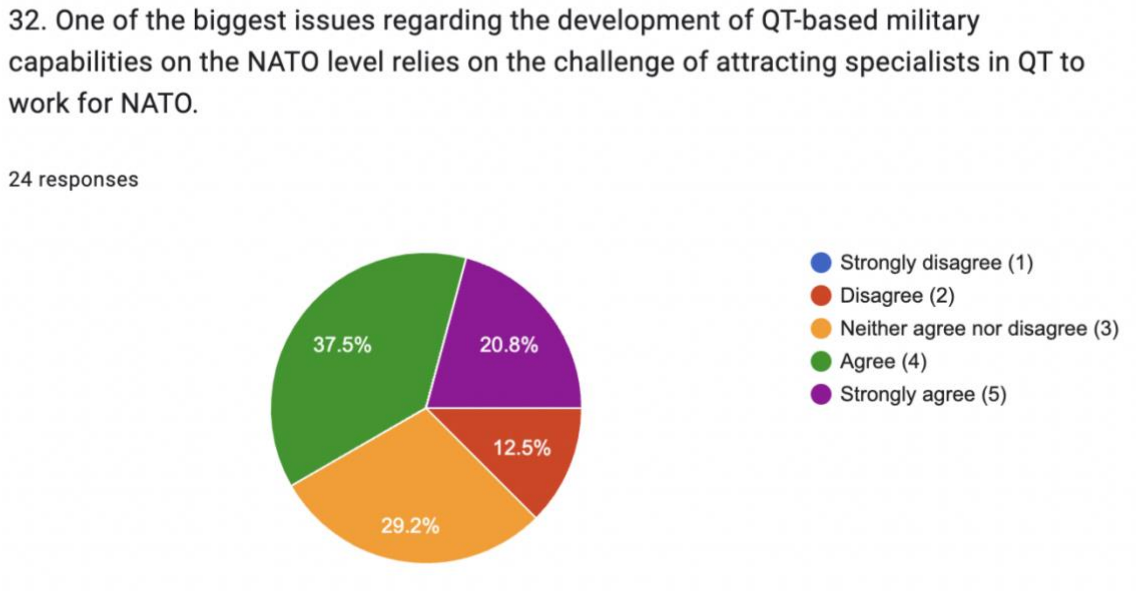


31. One of the biggest issues regarding the development of QT is the availability of enabling technologies and their ability to secure the supply chain [11].

[11] Here the author means the ability to build the competence among NATO nations, so they could produce their technologies independently from the rest of the world. E.g. quantum computers require precise metrology tools, secure manufacturing capabilities of specialised manufacturing and cryogenics.

24 responses

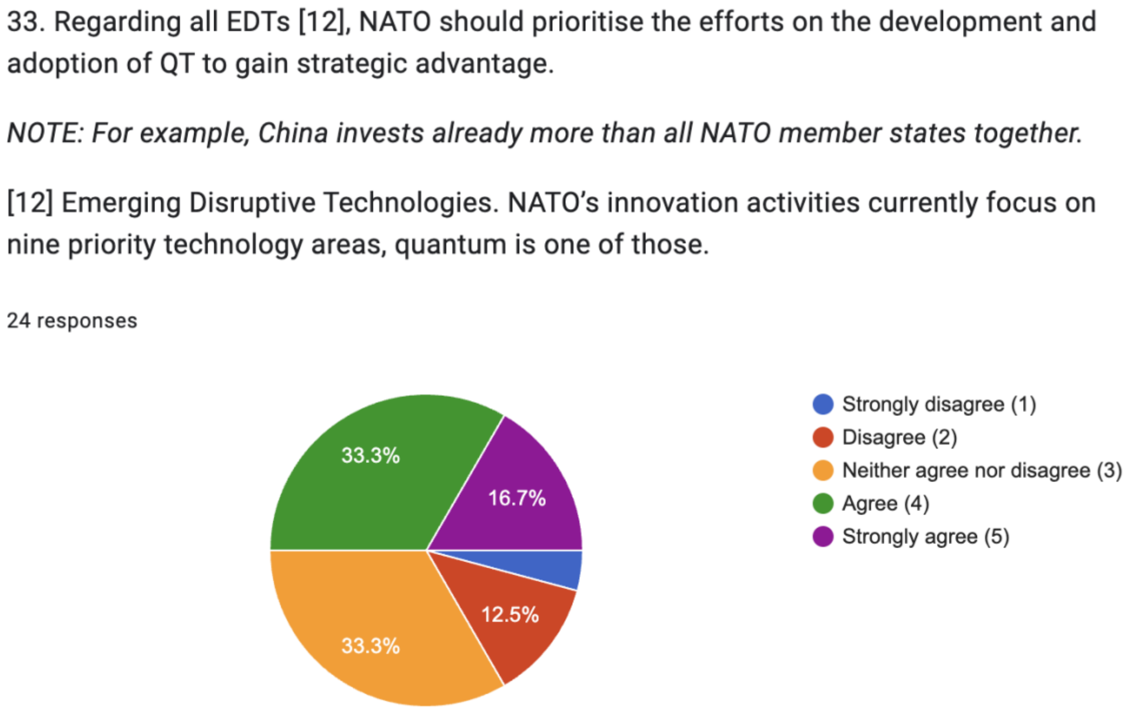
Figure 33. Responses to Statement 31



32. One of the biggest issues regarding the development of QT-based military capabilities on the NATO level relies on the challenge of attracting specialists in QT to work for NATO.

24 responses

Figure 34. Responses to Statement 32



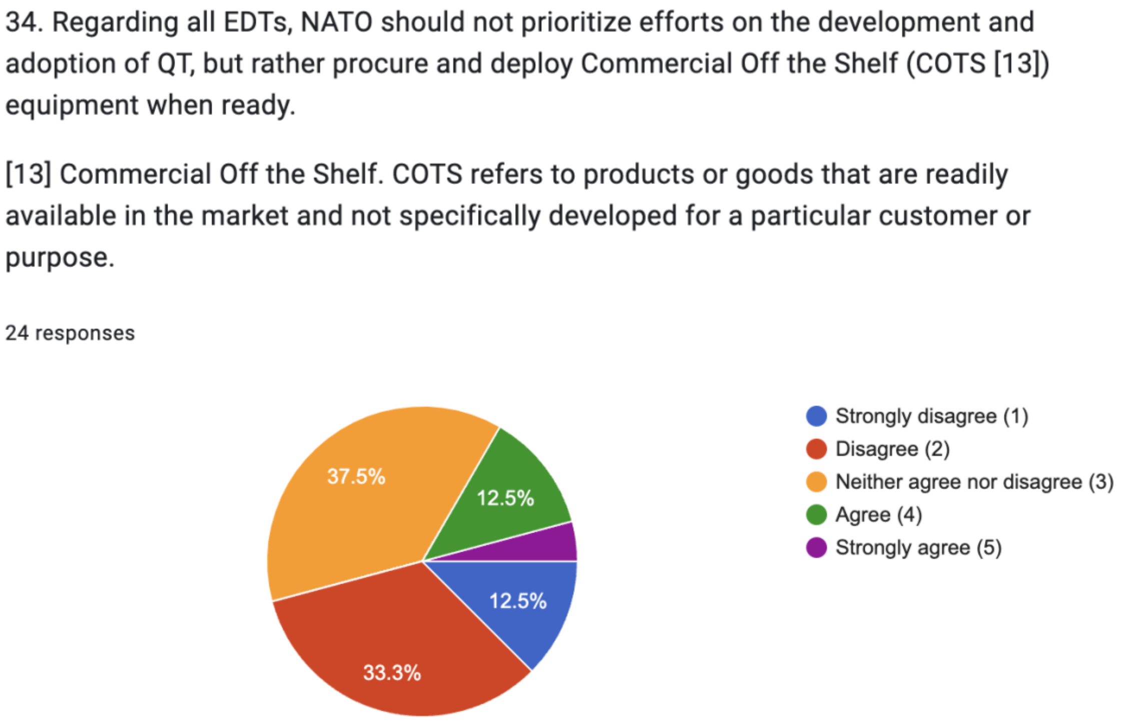
33. Regarding all EDTs [12], NATO should prioritise the efforts on the development and adoption of QT to gain strategic advantage.

*NOTE: For example, China invests already more than all NATO member states together.*

[12] Emerging Disruptive Technologies. NATO's innovation activities currently focus on nine priority technology areas, quantum is one of those.

24 responses

Figure 35. Responses to Statement 33



34. Regarding all EDTs, NATO should not prioritize efforts on the development and adoption of QT, but rather procure and deploy Commercial Off the Shelf (COTS [13]) equipment when ready.

[13] Commercial Off the Shelf. COTS refers to products or goods that are readily available in the market and not specifically developed for a particular customer or purpose.

24 responses

Figure 36. Responses to Statement 34

# 5 Analysis

In this chapter the data collected is analysed to determine the opinions and views of the respondents of the survey. Although the initial intention was to cover all topics that the statements covered individually, during the analysis process it became apparent that a different approach was needed. Subsequently, the data was grouped into different categories to better analyse the statements and responses received. Below are listed some of the main findings of the research:

1. There is a common opinion that QTs can bring opportunities to NATO and the Alliance. However, their disrupting effect on cybersecurity needs to be perceived as a weighted impact of opportunities and threats.
2. There is a common understanding that NATO should keep track on the current development of QT and start investing in these now. NATO may lose its technological advantage if it waits until the technology matures.
3. Quantum computers can help with cybersecurity analysis such as in pattern recognition for the detection of Advanced Persistent Threats (APTs).
4. Some practical use cases of the applications of QT are limited in the military context, such as QKD.
5. Some quantum experts believe that quantum communication will remain a niche for land-based communications, but perhaps an option for satellites.
6. Security standards of QT must be developed parallel with the development of new technologies.
7. Since NATO is an Alliance with its 32 countries, the Allies will move at different speeds in their deployment of QT.
8. NATO leaders and national defence representatives need training on QT in order to be able to integrate QT into the process of warfighting requirements identification, experimentation planning and execution, aligning future concepts with new potential capabilities.
9. The industry needs input from end users to understand what their requirements are. Therefore, NATO member states are best positioned to provide input into their own respective defence industrial base.
10. Many statements in this survey, especially regarding the challenges, can be used for other Emerging and Disruptive Technologies as well.

In order to better understand the insights, the respondents made in the survey the data was grouped into different categories. The details of responses have been presented in subsequent subchapters.

## 5.1 Opportunities and Threats of QT (Statements 1, 2, 3, 6)

According to statements 1, 2, 3 and 6, it can be said that the majority of people agreed that QT will affect NATO’s cybersecurity. 87,5% of quantum experts believed that QT will create opportunities and 62,5% believed that QT will improve the cybersecurity capabilities of the NATO Alliance. The respondents commented that QIS and its ability to solve specific hard computational problems can support modelling, simulation and optimization. This, linked with capabilities of QML (Quantum Machine Learning) and generative AI (LLMs – Large language Models) can for instance improve decision making in the area of cybersecurity (e.g. within the scope of DCO – Defensive Cyberspace Operations). QT can help with cybersecurity analysis, pattern recognition, and detection of APTs. Also, in the long term, it is expected that quantum computers has potential in optimising and QML, which can be used in the cyber domain. Enhancements on the security and privacy of communications recurring to stronger encryption methods and quantum security cryptography was mentioned as well.

For the 3rd statement, the respondents emphasized the risks and threats of QT to NATO's cybersecurity. There was similar to the response to the 3rd statement with 83,3% of the respondents agreeing that QT will also affect the future of cybersecurity by increasing the capability of threat actors. It was said that by demonstrating the theoretical vulnerabilities of some widely deployed public key cryptographic schemes, it has already changed the cybersecurity landscape. In future, the possible availability of quantum computers could offer many new opportunities to carry out attacks.The experts added that QT introduce a serious risk to the use of classical cryptography based on the difficulty of factoring large numbers or calculating discrete logarithms. It was added that there is competiton for nation-state actors to develop a CRQC that can potentially run Shor's algorithm. This may have already been developed, but has not been made public. That said, if it is or when it is available, it will be a significant development. Intelligence agencies will first target the highest valued information (highest classification strategic information) before using it to exploit time-perishable operational and tactical communications. In addition, it was mentioned that if NATO can't implement quantum resistant cryptographic solutions/standards, there might be severe consequences due to the ’’Harvest now, decrypt later” threat.

In the statement 6, the opinions varied. 70,8% of respondents believed that QT have potentially disruptive implications, which can degrade the NATO Alliance’s ability to deter and defend. Some believed that the quantum threat, can result in the compromise of NATO networks. However, others thought that QT will not trigger a game-changing revolution in military affairs as some are predicting, at least not at the moment.

## 5.2 HNDL and QKD (Statements 4, 5, 22, 23)

For statements 4 and 5, there was a strong common understanding. 83.4% of the respondents believed that HNDL attacks are already a threat to NATO. Even those who responded that they disagree, commented that this is already a threat to NATO, but they are not sure if it is the biggest one yet. Some of the respondents also emphasized that, based on a public information, it is proven that these attacks are happening now. The interesting fact that some people pointed out was that some of the data is only sensitive temporarily, therefore they did not consider HNDL attacks as a threat. However, some commented that NATO has some data that must remain secure for 25+ years, so HNDL is even bigger risk than it considered to be.

Regarding QKD, the opinions were very different. Overall, 50% of the experts disagreed with the 22nd statement that QKD is the best mitigation measure to become quantum safe. They added that it will probably become very suitable for a very limited set of use cases for military and for space even after it reaches maturity. Regarding the 23rd statement about quantum communications less than 50%, 46,6% believed that quantum communications will provide a significant improvement in secure communications. 37,5% neither agreed nor disagreed, this showed that there was no common opinion regarding this statement.

## 5.3 NATO and Its Activities (Statements 7, 8, 9, 25, 26, 27, 28, 29, 30, 32, 33, 34)

87,5% of the respondents agreed with the 7th statement. 100% of the respondents agreed with the 8th statement that NATO should keep track of what is currently being developed in terms of QT. There is also a strong common opinion that NATO should invest in QT already now. Regarding the 9th statement, 79,2% of the respondents said that NATO cannot wait until the technology is mature, because it will then be too late. The respondents commented that waiting for technology to mature leads to lack of expertise in the area when it is needed most. Also, that technology watch and application research are both urgent and important, especially regarding the military environment. Not taking action right now will result in a delay in the deployment compared to our opponents and potential gap in the Alliance capabilities. The statement is also supported by a comment stating that one key missions of NATO is conflict deterrence. Not taking a proactive approach won't be in alignment with that strength. Even the only one who disagreed with the statement did not exclude investing into QT, they just emphasized that first NATO should focus on facing the current challenges by investing in more traditional technologies rather than quantum. One person commented that QT will not make a difference on the battlefield for the next 10 years.

There was an even split between the respondents regarding the statement 25 that every NATO member state should have its own quantum strategy aligned with NATO's quantum strategy. There was a comment that member states provide the majority of NATO's capabilities, so they should focus on improving their QT capabilities themselves, including prioritising it via a dedicated quantum strategy. One respondent also pointed out that this has already been requested through the NATO Defence Planning Process. 6 respondents who disagreed with the statement added that NATO member states are different and not every country needs the QT strategy. Many respondents stated that the bigger countries such as France, the Netherlands, Germany, the US and UK require the strategy is necessary, but for smaller countries it is not essential.

Regarding the statement number 27, 79,1% of the respondents agreed that NATO nations could offer their quantum computer resources for NATO Operations. One person added that this could be included as a NATO Defence Planning Process target. Another person stated that quantum computing capabilities are necessary for NATO to develop its capabilities. In this case, the most efficient way would be to use the available quantum computing capabilities of one of NATO nations.

62,5% of the respondents agreed with the 28th statement, stating that NATO should create a Quantum Centre of Excellence (CoE) that can accelerate the development of QT tailored to military applications and promote the exchange of ideas among military personnel and Subject Matter Experts. The key concern of one respondent was that currently a lot of developments in QT are going on in many different places within NATO. Usually, alignment between actors is more coincidence and luck than policy. Therefore, this person believed that a Quantum CoE could help improve both coordination and the Alliance's knowledge base. Also, such a centre could speed up the process of collaborative work on military applications of QT. Many respondents emphasized DIANA, its activities and necessity. They believed that existing CoE-s should consider how QT can support their areas of expertise and let DIANA address the support for the more generic development of QT. One person pointed out that the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is already conducting work on quantum computing, emphasizing that the scope of their work should be further investigated.

According to the statement number 29, 83,4% of the respondents agreed or strongly agreed that NATO should broker opportunities made possible by QT with industry, governments, and end users, to foster the scaling up and adoption of QT to accelerate the development of QT-based military applications. One example was the development of the Transatlantic Quantum Community. The experts added their comments stating that without the exchange of ideas and acceleration of development among NATO nations it will be difficult to minimize the gap between the quantum capabilities of NATO, Allied Nations and non-NATO nations. It was also added that this is a good initiative, but it is important to not reinvent the wheel and to keep track of existing studies. NATO should promote the existing initiatives and then identify the shortfalls. Each nation should present their national programmes so that we can identify the synergies better. Of course, this is a sensitive topic and not everyone is keen to share. But there were also other opinions. Some of the experts thought that the development of QT has its own momentum independent of NATO’s influence. Also, it was added that it cannot be understood why NATO should be the right technology broker, other organizations could do that better.

66,6% of the respondents disagreed with the 30th statement that NATO should focus its investments on building a Fault-Tolerant Quantum Computer (FTQC). This was highlighted with the comment saying that the development of a FTQC does not fit within the role of NATO and the Alliance should not therefore invest in any aspect of it at all. The respondent said that it should be done by the individual nations as part of their research and development programs. If FTQC becomes available, NATO could consider investing in this capability if it has been identified to be useful in support of its efforts. Many respondents pointed out that NATO should instead focus its investments in getting ready for the introduction of quantum computers. For example, identifying the military problems where QT can be useful. It was emphasized that the development of FTQC should be the focus of big tech or member states; NATO should focus on the military applications of QT.

The comments to the previous statement led to the 32nd statement about the challenge of attracting specialists in QT to work for NATO. As in the previous statement, in this area, 58,3% of the respondents agreed that there is a lack of quantum experts and NATO should focus on training and hiring qualified people. Also, NATO should focus on training in the area of QT of their personnel on a level necessary to understand the application of these technologies. One person stated that NATO has a terrible branding problem with academics that its personnel usually doesn't know or care to admit. It was added that training and education of users, and decision makers is essential to implement QT and to attract also new people, as well as educating its internal workforce. In addition, there must be some cooperation between QT specialists and NATO to be able to plan the application of these technologies in particular military scenarios. One respondent believed that the bulk of the technology is developed within Nations and NATO does not need to attract specialists in the domain.

Exactly half of the respondents agreed with the 33rd statement that regarding all EDTs, NATO should prioritise the efforts on the development and adoption of QT to gain strategic advantage. It was highlighted that due to the answers to the previous statements, QT are one of the most important EDTs NATO should focus on. It was stated that QT are the most disruptive ones and should be a funding priority. This is particularly so if NATO emphasises the need to become a quantum ready Alliance, it should prioritize the adoption of QT. Many of the respondents believed that real disruptive technologies/systems will be a combination of several EDTs. Therefore, all EDTs should be supported. In the comments to this statement the importance of the cooperation with NATO, academia and industry was also emphasized several times. One of the respondents commented: "I think multiple efforts are needed to leverage EDTs. DIANA will not be sufficient all alone; it mostly addresses the start-up companies applying for challenges (with limited grants). National industry, academia and government agencies should work together. Multinational forums are very important to increase situational awareness. NATO study groups should be promoted to attract more SMEs from industry and academia. EDTs should be incorporated into NATO exercises and experiments".

Regarding the 34th statement "Regarding all EDTs, NATO should not prioritise the efforts on development and adoption of QT, but rather buy and deploy Commercial Off The Shelf equipment when ready", there were very different opinions. 37,5%, neither agreed nor disagreed with the statement and the second most popular answer was disagree (33,3%). According to the comments there was a strong opinion that NATO cannot wait for COTS, because it will be too late. The experts believed that QT need to mature before they can be realized, but keeping track of their development and awareness of what is available from the member states is certainly a requirement. Without additional effort, industry will offer COTS products not tailored to operational environment, which will make it difficult to use it in military applications. Therefore, it was highlighted that NATO military organizations should be willing to be a part of the product development to make the eventual transition easier.

## 5.4 Military Cooperation (Statements 15, 16)

Regarding the statements 15 and 16 were about the creation of process especially focused on the creation of QT applications in military domain. 62,5% of the respondents agreed with the statement that a process should be created especially focused on the creation of QT applications in the military domain. The respondents commented that although industry will move forward with QT research and deployment independent of military influence, the adaption of these technologies to military use cases would be necessary. They added that there should be attention paid to plan the evolution of QT development, verification and their implementation. Regarding the counter statement, 75% of the respondents disagreed that the process especially focused on the creation of QT applications in the military domain is not necessary and that commercial drive will be sufficient to fulfil capability gap. They commented that, QT scientists and QT companies have very little idea of military conditions and requirements and will not lead to satisfactory solutions or will not be fast enough. One respondent highlighted that military needs and commercial markets needs may not (and usually do no) overlap very easily for emerging technologies. Waiting for that would cause degradation of NATO's strategic edge. Another respondent found that the civilian sector will drive the development, but the defence sector should be involved to ease the transition when the technologies are ready.

## 5.5 Research (Statements 11, 12, 13, 14, 17, 18)

In the statement 11 it was said that NATO should increase the number of quantum companies taking part in DIANA initiatives. More than half, 14 people, 58,3% answered neither agree nor disagree. 8 people agreed and 2 people out of 24 disagreed with the statement. According to the results to this statement it can be said that expert did not have very strong common opinion about this topic. In the comments the respondents stated the following: “If the six companies are leading in the area, having those six companies involved could also be sufficient,” and also “First of all, we should define more precisely what Quantum Companies are. For example, IBM is well advanced in the field of Quantum Computers but is not a company which business is limited to QT nor they are central to their business portfolio yet. Second adding more of a specialty does not necessarily improve the quality of contributions. Last, I do not believe DIANA is limiting challenges to a specific set of specialties or companies. DIANA is setting a problem and expect any academia, institutions, Small and Medium Enterprises as well as major Defence players to respond”. It was added that 6 out of 44 is a reasonable number of quantum companies at this level of technology maturity. In some of the people opinion the involvement of quantum companies in DIANA accelerator should not be measured in terms of quantity, but quality. DIANA is to solve critical defence and security challenges, so that industry should understand what are the main challenges of QT/solutions applications in military operational conditions that are not common for civilian market. Publication of such challenges would speed up technology development and adaptation as well as lifting their technology readiness level. On the other hand, the respondents highlighted that to increase to number of companies can only be done if DIANA publishes challenges addressing QT in particular. Overall, it can be said that 6 companies out of 44 is a good number but in order to increase the number, DIANA has to prioritise quantum, provide requirements and involve the industry,

95,8% of the respondents agreed with the 12th statement about input from NATO member states for QT-based solutions. There was a strong common perspective for statements 12 and 13, that in order to produce QT-based solutions that are fit for military purposes, the industry needs input from NATO member states. Many respondents emphasized that the most important is the input from end users, not from strategists or general staff officers. It was added that products shall be developed with inputs from the militaries, and it is essential to work together in a successful triplet: academia, industry, defence (users). For this to work, defence users shall be trained and educated on the benefits of QT and how they can use them. It was also added that many of QT companies do not have a good understanding of the military context and the requirements to be battle-proof. Therefore, a military contribution is important to provide inputs and guidance in the development of QT applications for security and defence. One interesting aspect that was added from one respondent was that different nations have different geolocations; they have different environmental factors.

The statement number 14 was the following: "NATO should develop a process for supporting transition of QT from the lab to the operational environment." 66,7% or 16 people agreed with the statement. The experts commented that there are already existing processes that push for such transition. The longer-term aspects of the NATO Defence Planning Process, STO panel studies and the CNAD involvement with industry through the NIAG all contributes to support such a transition. Also, it was mentioned that the worst thing that NATO needs is yet another process. It has already too many, with very low effectiveness and poor added value for the war fighter. On the other hand, the respondents explained that currently most solutions are lab solutions, and the industry needs support from NATO in the last step of field deployability. They emphasized that this is critically important message and NATO has a convening power regarding this matter by bringing parties in the supply chain, including end users, together. Also, NATO should support transition by providing standards and validation mechanisms, like testbeds. This will inform QT science and industry of the military requirements and lead to more quantum advantage. Also, it will lower the risk for industry to adopt QT, as standards provide clarity on the desirable end product.

The statement number 17 said: “In order to increase the Technology Readiness Level (TRL) of QT that have potential to create strategic advantage, the most important aspect for NATO is cooperation with academia.” The majority, 41,7% of the respondents neither agreed nor disagreed with the statement, 25% agreed or strongly agreed and 33,3% disagreed with the statement. Regarding this statement the experts emphasized the tripartite cooperation between NATO, academia and industry. Their comments were the following: “I wouldn't say most important, academia-industry-military integration might be a better suit”, “Academia operates at lower TRL levels, and it is the companies that bring these levels higher. I would focus on start-ups or companies that work on academic outputs” Also “Academia is one player; industry is another, equally or even more important player’. In addition, “The gap between academic research and military operational realities is too big. NATO should focus on being able to collaborate effectively with larger private companies”. On the contrary it was said that the most important aspect for NATO is the cooperation with its member states, with would include its academic institutions and industry.

The next statement, statement number 18 was similar to the previous one, but this was about the cooperation with the industry. As it was seen from the comments for the previous statement, the experts tend to believe more in the cooperation with the industry instead of academia. There was a tie between two responses – agree and neither agree nor disagree, both with 41,7% of the respondents. But in this case, the experts rather agreed, 54,2% of the respondents to be precise. Although it still seems a bit unclear what the best approach would be, but most of the answers in it was emphasized that both industry and the academia are of similar importance and have a big role to play in the development process.

## 5.6 Implementation of QT (Statements 20, 21, 31)

The 20th statement was about post-quantum cryptography (PQC) as the best mitigation measure to become quantum-safe. Exactly 50% of the respondents neither agreed nor disagreed with the statement. It can be explained with a fact that many of the respondents commented that do not consider themselves as experts on this topic or they do not have enough expertise in this field. Thus, they did not have a strong opinion regarding this statement. The other half had very different opinions, but 20,8% and 12,5% of the experts rather agreed or strongly agreed with this statement. The respondents pointed out that other alternatives, like QKD only offer a partly solution, thus PQC would be better option, it is also the best for digital signatures. Many of the respondents believed that the best mitigation measure depends on the application. Overall, the experts thought that PQC is not mature yet, but once it's mature, it can be used very successfully as a mitigation measure. However, there was a common opinion that a hybrid solution must be used meaning that QKD shall be complemented with QKD.

This statement led to the statement number 21 about hybrid solution as the best mitigation measure. Regarding this statement, there was a tie between the responses "Agree" and "Neither agree nor disagree", both having 37,5% of the respondents. In total, exactly 50% of the respondents agreed or strongly disagreed with the statement. The experts commented that this is a reasonable approach and as for now, hybrid approaches seem the best, especially for the key exchange. However, the experts highlighted that a hybrid approach is not supported by many national security agencies (NSA), and this is not standardized yet. Many of those who chose to neither agree nor disagree stated again, that this is outside their area of expertise, and thus they didn't want to share their opinion.

The statement number 31 said the following: "One of the biggest issues regarding the development of QT is the availability of enabling technologies and their ability to secure the supply chain". In total 66,7% of the respondents agreed with the statement. In addition, there was a tie between strongly agree and neither agree nor disagree with 29,2% of responses. Even if the experts were not sure, if it is the main issue regarding the development of QT, they agreed that this is an issue that need to be solved as soon as possible.

## 5.7 Future of QT (Statements 10, 19, 24)

50% of the respondents agreed with the 10th statement saying that NATO could effectively use QT in its military operations in 2030 the earliest. A high number, 41,7% of respondents, who neither agreed nor disagreed explained that they really cannot predict the timeframe. 2 people out of 24 believed that year 2030 would be too early, if at all, to be ready for training. They predicted that the effective use of QT in military operations will happen in 2035 the earliest. The majority of respondents said that this will happen earlier, depending on a technology in particular. It was mentioned that a lot of quantum computing applications depend on the timeline of useful quantum computers. Also, if possible and available, NATO shall be using quantum enabled technologies by then. Possibly the most mature capability would be quantum-cryptography.

Regarding the statement number 19 about quantum resistant solutions, the 33,3% neither agreed nor disagreed with the statement, but 37,5% of the respondents tended to disagree. The experts commented that quantum resistant solutions are already appearing in the market. The respondents added that mature quantum-resistant solutions will be available within a few years, but adoption within the Alliance is likely to stretch well beyond 2030. It was also added that there is the possibility that Post Quantum Cryptography schemes and some QKD applications could be ready before 2030. One respondent highlighted that THALES has proposed post-quantum cryptography selected by NIST, but for the next phase they have to prepare to test the robustness of their code to attack by quantum computers.

Statement number 24 said: “NATO should implement an equitable transition of cryptographic systems to quantum-safe cryptography by 2030”. In total the majority, 70,8% of the experts strongly agreed or agreed with the statement. Some of the respondents highlighted that it should be done by 2030 or beyond, once quantum safe cryptography has proven and is available. However, some respondents said that the transition should happen earlier, the sooner the better and we should plan for the transition already today. One of the respondents added that for key-exchange, NATO should aim for 2030. However, he sees lack of initiatives on this matter. For digital signatures, 2030 is probably too soon, as he does not expect any proper QR PKI (public key infrastructure) solution to be ready and its adoption by the PKI clients. One of the respondents commented that this idea of the statement is great, however first we need standards, then synchronisation across these standards, then synchronisation across all member states PQC recommendations, and then STANAG (NATO Standardization Agreement).

# 6 Discussion

This chapter presents the opinions and conclusions of the author, based on the analysis of the literature and survey results.

## 6.1 Discussion of the Main Findings

1. There is a common opinion that QT can bring opportunities to NATO and the Alliance. However their disrupting effect on cybersecurity needs to be perceived as a weighted impact of opportunities and threats.

According to respondents, QT, especially quantum computing can bring great opportunities to defense applications. However, concerning cybersecurity, the quantum threat and the possibility of threat actors using quantum computing capabilities against NATO are seen as significant risks. This could disrupt the operation of the Alliance in the next 5-10 years. It can be seen already now that QT are already a threat to NATO, taking into accound HNDL attacks.

2. There is a common understanding that NATO should keep track on the current development of QT and start investing in these now. NATO may lose its technological advantage if it waits until the technology matures.

The pace of development is dynamic and non-linear. Sometimes scientific discoveries can speed up the process significantly or add to the well-known technology. One of the examples is quantum memory, that has speed up the process of building a quantum internet [112]. That is why it is crucial to perform continuous technology watch in order to be able to notice important rapid changes in the technology state of the art.

Investing in the technology does not necessarily mean procurement of the equipment, which is not mature yet. It means necessity to train as technology evolves and learn how to make the best use of it. Additionally, it is important to verify if the high TRL solutions available on the market are ready to be used in military use cases, especially in operations and missions. This requires creating synthetic environment to train and scenarios that reflect real operational needs. This concept to “learn by doing” can make it possible to verify the applicability of particular technologies during training, but also sometimes trigger new technical use cases that have not been foreseen before.

This is particularly true for the quantum computing which needs special formulation of hard problems offering the possibility to solve them efficiently. However, it is not easy to formulate the problem so that the quantum computer can solve if efficiently. Nor it is also to fit it into the available quantum algorithms range. That is why early experimentation with quantum computing can, on the one hand, make subject matter experts from different Communities of Interest (COIs), like Command and Control (C2) or JISR, learn to use quantum algorithms for their purposes. On the other, it can also speed up the process of development of new quantum algorithms.

3. Quantum computers can help with cybersecurity analysis such as in pattern recognition for the detection of Advanced Persistent Threats (APTs).

Quantum computers are seen by respondents as disruptive technology that can add up to the NATO cybersecurity capabilities. The respondents emphasised the field of pattern recognition that is important in the area of threat hunting and anomaly detection in different areas of cybersecurity. There is a whole set of problems related to pattern recognition and machine learning. Quantum computers can be efficient in optimization.

Quantum algorithms for optimization problems are relevant to military data processing applications. By using a quantum computer's ability to explore multiple solutions simultaneously, there is a possibility to develop efficient and effective algorithms that can provide optimal or near-optimal solutions, thereby enhancing operational efficiency and resource utilization in military missions. Quantum machine learning algorithms have the potential to revolutionize military intelligence and analysis, especially regarding pattern recognition, anomaly detection, and classification. By harnessing quantum properties such as superposition and entanglement, the efficiency and accuracy of machine learning algorithms can be enhanced, enabling faster and more effective analysis of (large-scale) data sets, including images, sensor data, and signal intelligence.

Another interesting area is data analysis and decision support, where QT can provide significant advantages in for military operations. The objective is to develop quantum algorithms for data mining, pattern extraction, predictive modelling, and decision-making under uncertainty. By leveraging a quantum computer's potential for parallelism and optimization, there is a possibility to expedite the analysis of large and complex data sets, enabling more informed and timely decisions on the battlefield.

4. Some practical use cases of the applications of QT are limited in the military context, such as QKD.

As for now the approach to quantum communications and QKD in particular, due to its immaturity to certify[1] the devices, high cost, low range for terrestrial links (without quantum repeaters) and unknown of the practical level of their security is pessimistic. This is especially clearly highlighted by the Cyber Security Authorities (like BSI, ANSII, etc.) in order to give guidance for the short-term mitigating actions with respect to the quantum threat. That is why the use cases that are currently seen as the most relevant for QKD are located in the space segment, between the satellites and ground stations.

Perception of the new key distribution technology based on quantum effects will be for sure changed when the architectural, design and security problems will be overcome. For instance, this would be beneficial to see QKD devices exchange keys with the speed similar to todays' fibre channel links, which would allow to use the OTP (One Time Pad) approach to encryption.

There are also other challenges to be overcome by the QKD systems, like: necessity to develop  repeaters/ trusted nodes; lack of authentication between nodes; necessity of common approach to certification of QKD devices in NATO; standardization of QKD protocols (e.g. BB84), necessity to develop secure and trusted "last mile" key distribution system – from the QKD device to the end device. This all makes it difficult to think that QKD can soon be the response to the quantum threat. Nevertheless, there is potential for QKD, together with further phases of quantum communications.

[1] A certification ecosystem for QKD products must be established, in which test criteria and evaluation methods are coordinated and further developed.

5. Some quantum experts believe that quantum communication will remain a niche for land-based communications, but perhaps an option for satellites.

As described above, maturity of quantum communications makes its applications in the current systems unlikely. However, its potential in satellite communications is perceived more optimistically than for terrestrial links (see discussion for point 5). This direction should be explored further as European Union is investing heavily in the QCI project developing European quantum communications infrastructure. This should be the playground for the Allies to learn about the true opportunities of these technologies, given the advancements in this area of other global players (like China).

6. Security standards of QT must be developed in parallel with the development of new technologies.

QT are under development and many technical challenges, sometimes from the basic science, need to be overcome in order to succeed. However, this is also the time to do research on their security, which is crucial for military applications.

For the devices that will process data (especially if planned to be used in unclassified networks) there has to be a certification process that will assess the risk of using particular device in a system of particular classification level. This encompasses verification of security proof, security of the software and hardware and existence of any possible attacks (also side – channel ones). Therefore, this holds e.g. for the QKD and quantum communication devices.

For quantum computers it is necessary to face challenges related e.g. to the following issues: trust to the results of computation, security of the interface between the classical computer and quantum part, security of the quantum computing software stack, creation of the anti-malware solutions.

Additionally, as quantum effects are vulnerable to e.g. decoherence, it is necessary to identify if the solutions discussed have weaknesses that may impact their applicability in military scenarios. These are related inter alia with possible scenarios focusing on: disrupting quantum communications, spoofing quantum sensors, or disabling quantum computers. Taking this into account NATO should focus its EDTs efforts on protection from threats to quantum technology which are associated with its weaknesses and possibility to be used intentionally by a threat actor.

7. Since NATO is an Alliance with its 32 countries, the Allies will move at different speeds in their deployment of QT.

Development of QT is very costly and makes it much easier for wealthy countries. This will create imbalance among NATO member states as some of them e.g. will not be able to afford building their own quantum computer. That’s why it is necessary to share these important resources among Allies and make them available to countries that cannot have so much spending on the R&D process. This holds e.g. for the quantum computing platforms which are already commercially available online.

Currently however QT are developed as dual-use ones, mainly by commercial companies, which makes it difficult to influence their future path. That is why creation of any specialized quantum computer, tailored to military purposes, would make it necessary to create tight cooperation with one of the tech companies.

8. NATO leaders and national defence representatives need training on QT in order to be able to integrate QT into the process of warfighting requirements identification, experimentation planning and execution, aligning future concepts with new potential capabilities.

QT is a new emerging disruptive technology. Despite the fact, that quantum has been here already for some time, it is still a new and unknown technology, especially for the military field. It is important not to focus only on risks, but also the opportunities of QT. It means that in order to actually implement QT in the future, training is essential to get to know the operational relevance of each solution, also under special harsh conditions, adversarial threats and dynamics of actions, and be able to plan and best fit the use of QT in different use cases.

9. The industry needs input from end users to understand what their requirements are. Therefore, NATO member states are best positioned to provide input into their own respective defence industrial base.

One of the biggest challenges regarding the development of QT is the mismatch between the needs and offer. The reason behind it is the lack of necessary dialogue in order to find out the real needs and matching offer. In order to foster stronger cooperation between the industry and end-users, NATO should implement a bottom-up approach, meaning, that all member states can work together with their country's companies.

10. Many statements in this survey, especially regarding the challenges, can be used for other Emerging and Disruptive Technologies as well.

The respondents to the survey mentioned several times that similar or the same issues can be addressed regarding all the other EDTs. Not depending on the EDTs, the issues and challenges are the same.

## 6.2 Discussion of the Research Questions

It can be seen from the research that quantum experts generally agree on the disruptive nature of QT. Within the scope of security and defence quantum threat is seen as crucial aspect. They also universally agree on the necessity to create a process for QT development for military applications. It was stated that QT will be very disruptive for NATO in the future, and they will affect NATO's cybersecurity in both the short and long term. Currently, QT are considered as a threat to NATO, but it also has some advantages.

In **RQ1** it was asked: "What QT are seen as threats and opportunities to NATO's cybersecurity how can they influence the security posture of NATO's communications and information systems (CIS)?"

Regarding all QT, in terms of cybersecurity there are two main technologies that have relevance to NATO's CIS infrastructure – quantum computing and quantum communication. They can influence NATO's security posture in a positive and a negative way.

Regarding NATO's security posture quantum computing is the enabling technology for implementation of the Shor's and Grover's algorithms and breaking current encryption schemes. Moreover, QT provides the opportunity to improve computational capabilities, wargaming and simulations, also enhance faster decision making. QT can also help with cybersecurity analysis, especially in pattern recognition and threats detection.

**RQ2** investigated "What should NATO do in order to support the development of QT for military applications to protect the Alliance?". One of the main findings was the importance of trilateral dialogue between NATO, industry, and academia. In order to support the process of QT development, this should be ongoing. The experts who participated in the research repeatedly emphasized that industry and academia do not really understand what the needs of end-users are. End-users in turn do not know what to ask for, because they do not know what the industry can offer.

Member states also have their role to play in this, meaning that their companies can work on developing new technologies and quantum computing capabilities.

NATO consists of 32 member states that have very different capabilities in QT. In order to harmonize the development and use of QT, national quantum strategies aligned with NATO's strategy should be created and implemented in order to support all member states. Also, establishment of Quantum Centre of Excellence should be considered as well.

Another very important topic that had a common understanding was concerning the supply chain. In particular it was determined that some of the global players have better access to raw materials used in the production of quantum technologies than NATO countries. The activities and policies of these states limit NATO members access to CRMs that are vital for the development of QT. Experts who participated in the research pointed out that in order to develop dual-use quantum technologies and protect the market, it is essential to secure the supply chain.

**RQ3** addressed "What are the indicators that could guarantee NATO quantum readiness?". There are several ways how NATO could become quantum-ready. It was determined that NATO should invest in quantum now not wait until the technology is mature. First of all, it should be mentioned that more emphasis should be put on fostering all the opportunities to apply quantum technologies where they can bring positive impact on security and defence.

In addition to opportunities, due to the possibility of the HNDL attacks, NATO should place the emphasis on risk mitigation. Quantum threats to classical cryptography requires mitigation measure to limit the quantum threat and implement post-quantum cryptography. NATO should implement an equitable transition of cryptographic systems to quantum-safe cryptography by 2030. In parallel with post-quantum cryptography, NATO should also work on implementing QKD. It should be taken into account that QKD can be used only for some niche applications, but this can be an important technology for future communication.

# 7 Areas for Future Research

There are many opportunities for future research regarding this thesis. As was discovered during this research the knowledge of the opportunities of QT in relation to security and defence is currently still difficult to assess. The technology needs to mature as well as understanding of the topic and the ways to use available and future solutions in military operations needs to be created among the military personnel of all levels of command.

Future research should focus on specific QT – either quantum computing, communication or cryptography. In this research the applications and use cases of particular QT should be investigated.

Future research could repeat the same Delphi method, but by doing several rounds not only one that was done in this research. In this case there will be an opportunity to see if the experts can agree on one common opinion. Another opportunity for future research could be done by using DOTMLPF-I analysis that was also considered as a research method for this thesis.

In addition, the future research could incorporate a comparison between NATO and its contenders, e.g. China and Russia. This study would be valuable in determining the relative strength of NATO and its adversaries. However, this research would involve access to classified material and would be for NATO internal use only.

# 8 Conclusion

This paper covers various threats and opportunities that QT pose. Quantum computing has the potential to bring exciting new capabilities to the NATO Alliance. Investing in QT must be part of NATO's ongoing commitment to innovation and capability development.

The data collected proved to be of value to NATO and the Member States' community, because it was provided by the experts both in the area of QT and NATO (see Table 2). This intersection gives truly unique point of view that gives a strategic insight into the future of QT in cybersecurity of NATO. Also, the value behind this research is that the respondents were people from all three sectors – academia, industry and NATO. Therefore, it can be said that there were representatives from the researcher until end-user side.

This research identified that industry needs greater communication from NATO and NATO member states in particular. The dialogue between the industry, academia and NATO is essential, because if that isn't properly undertaken there will be both an inefficient use of resources and the creation of a sub-optimal products.

In order to manage the transition to quantum-safe infrastructure and cryptographic tools, a proactive approach to quantum cybersecurity needs to be fostered. This will help to reduce risk associated with hasty transitions motivated by crisis.

As a result of this research the following recommendations have been made (see Table 3 below) as to how NATO could manage the quantum risk and ensure its smooth transition to become quantum-ready Alliance.

Table 3. Recommendations for NATO to Become Quantum-Ready Alliance

| **Short-term goals (5 years)** | **Mid-term goals (10 years)** | **Long-term goals (20 years)** |
|---|---|---|
| Ongoing and continuous technology watch. | Member states offer their QC resources to NATO Allies. | Implementation of quantum communication. |
| Development of national quantum strategies. | Establishing Quantum Centre of Excellence. | |
| PQC and quantum computing (QC) | | |
| Implementation of PQC and hybrid approach. | | |
| Development of QC use cases for military domain.<br>Research on security and trust mechanisms to the computational process. | Exercising and implementation of early QC use cases for military domain. Early implementations of security and trust to the computational process. | Implementation of QC use cases for military domain. Medium and/or mature implementations of security and trust to the computational process. |
| Development of quantum clocks. | | |
| Development of QRNGs. | | |
| | QKD vulnerabilities/ opportunities | QKD implementation |
| Development of process focused on application of QT in military domain (e.g. using DIANA). | DIANA challenges related to QT. | |
| Fostering the collaboration within Transatlantic Quantum Community. | | |
| Experimentation with QC algorithms. | maturing | implementation |
| Including NATO member states/end-users input into QT development process in the industry. | | |
| Securing the supply chain | | |

# References

[1] V. Silva, “Practical Quantum Computing for Developers,” Apress, 2018. [Online]. Available: https://link.springer.com/book/10.1007/978-1-4842-4218-6. [Accessed 18 09 2023].

[2] M. Krelina, “Quantum technology for military applications,” 06 11 2021. [Online]. Available: https://epjquantumtechnology.springeropen.com/articles/10.1140/epjqt/s40507-021-00113-y. [Accessed 01 08 2023].

[3] A. Udal, “Kolmas kvantrevolutsioon: kvantarvutite tulekuga kaasnevad probleemid ja võimalused,” *Pikksilm,* 21 02 2020.

[4] G. Press, “27 Milestones In The History Of Quantum Computing,” Forbes, 18 05 2021. [Online]. Available: https://www.forbes.com/sites/gilpress/2021/05/18/27-milestones-in-the-history-of-quantum-computing/?sh=3bc8a697b23f. [Accessed 09 02 2024].

[5] NATO Science & Technology Organization, “Science & Technology Trends. Exploring the S&T Edge,” 03 2020. [Online]. Available: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf. [Accessed 02 09 2024].

[6] “10 THINGS YOU NEED TO KNOW ABOUT NATO,” NATO, 11 03 2024. [Online]. Available: https://www.nato.int/cps/en/natohq/126169.htm. [Accessed 02 05 2024].

[7] “NATO Exploring Quantum Technology for Future Challenges,” 14 10 2022. [Online]. Available: https://www.act.nato.int/article/nato-exploring-quantum-technology-for-future-challenges/. [Accessed 01 08 2023].

[8] “Summary of NATO’s Quantum Technologies Strategy,” NATO, 16 01 2024. [Online]. Available: https://www.nato.int/cps/en/natohq/official_texts_221777.htm. [Accessed 09 02 2024].

[9] “NATO releases first ever quantum strategy,” NATO, 17 01 2024. [Online]. Available: https://www.nato.int/cps/en/natohq/news_221601.htm?selectedLocale=en. [Accessed 29 01 2024].

[10] World Economic Forum, “State of Quantum Computing: Building a Quantum Economy,” 2022. [Online]. Available: https://www3.weforum.org/docs/WEF_State_of_Quantum_Computing_2022.pdf. [Accessed 22 01 2024].

[11] K. Kwon, “China Reaches New Milestone in Space-Based Quantum Communications,” Scientific American, 25 06 2020. [Online]. Available: https://www.scientificamerican.com/article/china-reaches-new-milestone-in-space-based-quantum-communications/. [Accessed 06 02 2024].

[12] M. Mosca and M. Piani, “2023 Quantum Threat Timeline Report,” Global Risk Institute, 22 12 2023. [Online]. Available: https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/. [Accessed 30 01 2024].

[13] “Cyber defence,” NATO, 14 09 2023. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_78170.htm. [Accessed 20 04 2024].

[14] NATO Science & Technology Organization, “Science and Technology Trends 2023-2043. Volume 1: Overview,” NATO Science and Technology Orgnisation, Brussels, 2023.

[15] “NATO 2030,” NATO, [Online]. Available: https://www.nato.int/nato2030/index.html.

[16] “Defence Innovation Accelerator for the North Atlantic (DIANA),” NATO, 26 09 2023. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_216199.htm. [Accessed 20 04 2024].

[17] “NATO 2030 Factsheet,” NATO, 06 2021. [Online]. Available: https://www.act.nato.int/wp-content/uploads/2023/05/2106-factsheet-nato2030-en.pdf. [Accessed 23 02 2024].

[18] D. Mandich, “This silent cyber threat is a ticking time bomb,” Security Info Watch, 21 09 2023. [Online]. Available: https://www.securityinfowatch.com/cybersecurity/article/53073055/this-silent-cyber-threat-is-a-ticking-time-bomb. [Accessed 13 04 2024].

[19] The White House, “Executive Order on Enhancing the National Quantum Initiative Advisory Committee,” 04 05 2022. [Online]. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/05/04/executive-order-on-enhancing-the-national-quantum-initiative-advisory-committee/. [Accessed 12 04 2024].

[20] The White House “National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems,” 04 05 2022. [Online]. Available: https://www.whitehouse.gov/briefing-

room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/. [Accessed 20 04 2024].

[21] S. Schlarman, “The People, Policy, Technology (PPT) Model: Core Elements of the Security Process,” Information Systems Security, 21 12 2006. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1201/1086/43315.10.5.20011101/31719.6. [Accessed 02 05 2024].

[22] NATO Science & Technology Organization, “Science & Technology Trends 2023-2043, Volume 2: Analysis,” 03 2023. [Online]. Available: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf. [Accessed 23 04 2024].

[23] National Academies of Sciences, Engineering, and Medicine, “Quantum Computing: Progress and Prospects,” 2019. [Online]. Available: https://nap.nationalacademies.org/catalog/25196/quantum-computing-progress-and-prospects. [Accessed 29 01 2024].

[24] IBM Institute of Business Value, “The Quantum Decade. A playbook for achieving awareness, readiness and advantage. Third Edition.,” IBM Corporation, 2022. [Online]. Available: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/quantum-decade. [Accessed 26 02 2024].

[25] IBM, “What is quantum computing?,” [Online]. Available: https://www.ibm.com/topics/quantum-computing. [Accessed 28 08 2023].

[26] The Quantum Atlas, “Quantum Entanglement,” [Online]. Available: https://quantumatlas.umd.edu/entry/entanglement/. [Accessed 02 05 2024].

[27] M. Krelina, “The Prospect of Quantum Technologies in Space for Defence and Security,” Elsevier, 08 2023. [Online]. Available: https://doi.org/10.1016/j.spacepol.2023.101563. [Accessed 26 02 2024].

[28] F. D. Kramer, A. M. Dailey and J. Brodfuehrer, “NATO multidomain operations: Near- and medium-term priority initiatives,” Atlantic Council, 21 02 2024. [Online]. Available: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/nato-multidomain-operations/. [Accessed 04 05 2024].

[29] R. Konik, “Quantum coherence confined.,” Nature Physics, 18 03 2021. [Online]. Available: https://doi.org/10.1038/s41567-021-01211-5. [Accessed 02 05 2024].

[30] N. V. Patel, “Cosmic rays could pose a problem for future quantum computers,” MIT Technology Review, 26 08 2020. [Online]. Available: https://www.technologyreview.com/2020/08/26/1007688/cosmic-rays-could-pose-a-problem-for-future-quantum-computers/. [Accessed 22 04 2024].

[31] “40 years of quantum computing,” Nature reviews physics , 10 01 2022. [Online]. Available: https://doi.org/10.1038/s42254-021-00410-6. [Accessed 02 04 2024].

[32] W. D. Oliver, “Quantum Computing takes flight,” Nature, 23 10 2019. [Online]. Available: https://www.nature.com/articles/d41586-019-03173-4. [Accessed 23 02 2024].

[33] S. Feldman, “20 Years of Quantum Computing Growth,” Statista, 06 05 2019. [Online]. Available: https://www.statista.com/chart/17896/quantum-computing-developments/. [Accessed 05 09 2023].

[34] F. Arute, K. Arya, R. Babbush, D. Bacon and e. al, “Quantum supremacy using a programmable superconducting processor,” Nature, 23 10 2019. [Online]. Available: https://www.nature.com/articles/s41586-019-1666-5. [Accessed 05 09 2023].

[35] ATARC, "Applied Quantum Computing for Today's Military," Advanced Technology Academic Research Center, 05 2021. [Online]. Available: https://atarc.org/wp-content/uploads/2021/05/ATARC-Military-Paper-by-Quantum-Working-Group.pdf#:~:text=Applied%20quantum%20computing%2C%20which%20can%20be%20enriched%20by,real-time%20or%20near%20real%20time%20analysis%20to%20commanders.. [Accessed 11 09 2023].

[36] “Technology for the quantum future,” IBM Quantum, [Online]. Available: https://www.ibm.com/quantum/technology. [Accessed 20 04 2024].

[37] “Our quantum computing journey,” Google, [Online]. Available: https://quantumai.google/learn/map. [Accessed 20 04 2024].

[38] J. Preskill, “Quantum Computing in the NISQ era and beyond,” 30 07 2018. [Online]. Available: https://arxiv.org/pdf/1801.00862.pdf. [Accessed 06 02 2024].

[39] M. H. Devoret and R. J. Schoelkopf, “Superconducting Circuits for Quantum Information: An Outlook,” Science, 08 03 2013. [Online]. Available: https://www.science.org/doi/10.1126/science.1231930. [Accessed 23 04 2024].

[40] P. Kealey and M. Serna, “Quantum Capabilities for Sensing and Communications - Summary Report,” Von Kármán Horizon Scanning, 20 09 2018. [Online]. [Accessed 02 05 2024].

[41] D. Jones, “Quantum Mania: How Quantum Computing Will Affect Your Cybersecurity,” Mimecast, 19 09 2023. [Online]. Available: https://www.mimecast.com/blog/quantum-mania-how-quantum-computing-will-affect-your-cybersecurity/. [Accessed 16 02 2024].

[42] Federal Office of Information Security , “Quantum-safe cryptography – fundamentals, current developments and recommendations,” 10 2021. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=4. [Accessed 25 04 2024].

[43] F. Beato, A. Ardon, I. Barmes and C. Knackstedt, “Transitioning to a Quantum-Secure Economy,” World Economic Forum, 13 09 2022. [Online]. Available: https://www.weforum.org/publications/transitioning-to-a-quantum-secure-economy/. [Accessed 20 04 2024].

[44] P. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” 20 11 1994. [Online]. Available: https://ieeexplore.ieee.org/document/365700. [Accessed 12 04 2024].

[45] R. Davis, “It’s been 20 years since “15” was factored on quantum hardware,” IBM, 26 01 2022. [Online]. Available: https://www.ibm.com/quantum/blog/factor-15-shors-algorithm. [Accessed 12 04 2024].

[46] T. L. Scholten, C. J. Williams, D. Moody, M. Mosca, W. Hurley, W. J. Zeng, M. Troyer and J. M. Gambetta, “Assessing the Benefits and Risks of Quantum Computers,” 30 01 2024. [Online]. Available: https://arxiv.org/pdf/2401.16317.pdf. [Accessed 06 02 2024].

[47] P. Lipman, “How Quantum Computing Will Transform Cybersecurity Forbes Technology Council Paul Lipman,” Forbes, 04 01 2021. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2021/01/04/how-quantum-computing-will-transform-cybersecurity/?sh=4d1cc9537d3f. [Accessed 04 01 2023].

[48] N. M. P. Neumann, M. P. van Heesch and P. de Graaf, “Quantum Communication for Military Applications,” 11 2020. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/2011/2011.04989.pdf. [Accessed 04 02 2024].

[49] M. Giles, “Explainer: What is quantum communication?,” MIT Technology Review, 14 02 2019. [Online]. Available: https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/. [Accessed 12 04 2024].

[50] ANSSI, “ANSSI views on the Post-Quantum Cryptography transition,” 30 09 2022. [Online]. Available: https://cyber.gouv.fr/publications/anssi-views-post-quantum-cryptography-transition?preview=true&preview_id=29603&preview_nonce=b338a6a657. [Accessed 31 01 2024].

[51] D. Hurley, “The Quantum Internet Will Blow Your Mind. Here’s What It Will Look Like,” Discover, 04 10 2020. [Online]. Available:

https://www.discovermagazine.com/technology/the-quantum-internet-will-blow-your-mind-heres-what-it-will-look-like. [Accessed 12 04 2024].

[52] W. Diffie and M. E. Hellman, “New Directions in Cryptography,” IEEE Transactions on Information Theory, 11 1976. [Online]. Available: https://ee.stanford.edu/~hellman/publications/24.pdf. [Accessed 03 05 2024].

[53] U. Maurer, “Information-Theoretic Cryptography. dvances in Cryptology — CRYPTO' 99. Lecture Notes in Computer Science.,” 08 1999. [Online]. Available: https://link.springer.com/chapter/10.1007/3-540-48405-1_4. [Accessed 03 05 2024].

[54] Quantum Delta NL, “Exploratory Quantum Technology Assessment,” Quantum Delta NL, 14 04 2023. [Online]. Available: https://quantumdelta.nl/news/quantum-delta-nl-launches-exploratory-quantum-technology-assessment-eqta. [Accessed 02 05 2024].

[55] E. Parker, “Commercial and Military Applications and Timelines for Quantum Technology,” RAND Corporation, 2021. [Online]. Available: https://www.rand.org/pubs/research_reports/RRA1482-4.html.

[56] C. C.-W. Lim and C. Wang, “Long-distance quantum key distribution gets real,” Nature Photonics, 06 07 2021. [Online]. Available: https://www.nature.com/articles/s41566-021-00848-1. [Accessed 14 04 2024].

[57] “What is Quantum Cryptography (or Quantum Key Distribution)?,” ID Quantique, [Online]. Available: https://www.idquantique.com/quantum-safe-security/quantum-key-distribution/. [Accessed 04 05 2024].

[58] M. Swayne, “PacketLight, ID Quantique Announce Successful Integration Of Quantum Key Distribution In PacketLight Devices,” The Quantum Insider, 07 09 2023. [Online]. Available: https://thequantuminsider.com/2023/09/07/packetlight-id-quantique-announce-successful-integration-of-quantum-key-distribution-in-packetlight-devices/. [Accessed 02 05 2024].

[59] M. Swayne , “Toshiba Europe And Single Quantum Partner To Provide Extended Long-Distance QKD Deployment Capability,” The Quantum Insider, 23 04 2023. [Online]. Available: https://thequantuminsider.com/2024/04/23/toshiba-europe-and-single-quantum-partner-to-provide-extended-long-distance-qkd-deployment-capability/. [Accessed 02 05 2024].

[60] Quantum Internet Alliance, “D4.1 Quantum Applications and Use Case Report,” Quantum Internet Alliance, 22 12 2020. [Online]. Available: https://quantum-internet.team/wp-content/uploads/sites/3/2022/05/D4.1-Quantum-Applications-and-Use-Case-Report.pdf. [Accessed 25 04 2024].

[61] S. Wehner, D. Elkouss and R. Hanson , “Quantum internet: A vision for the road ahead,” Science, 19 10 2018. [Online]. Available: https://www.science.org/doi/10.1126/science.aam9288. [Accessed 22 04 2024].

[62] ID Quantique, “QUANTUM-SAFE SECURITY WHITE PAPER,” ID Quantique, 05 2020. [Online]. Available: https://marketing.idquantique.com/acton/attachment/11868/f-020d/1/-/-/-/-/Understanding%20Quantum%20Cryptography_White%20Paper.pdf. [Accessed 02 05 2024].

[63] NATO, “Quantum computing and the threat to network security,” *NITECH,* no. 9, pp. 26-27, 07 2023.

[64] M. v. Amerongen, “Quantum technologies in defence & security,” NATO, 03 06 2021. [Online]. Available: https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html.

[65] French Cybersecurity Agency (ANSSI), Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA), Swedish National Communications Security Authority, Swedish Armed Forces, “Position Paper on Quantum Key Distribution,” 26 01 2024. [Online]. Available: https://cyber.gouv.fr/en/actualites/uses-and-limits-quantum-key-distribution. [Accessed 12 04 2024].

[66] “Quantum Key Distribution (QKD) and Quantum Cryptography (QC),” National Security Agency/ Central Security Service, 2020. [Online]. Available: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/. [Accessed 20 04 2024].

[67] “The European Quantum Communication Infrastructure (EuroQCI) Initiative,” European Commission, 18 04 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci. [Accessed 27 04 2024].

[68] European Commission, “New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient,” European Commission, 16 12 2020. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391. [Accessed 22 04 2024].

[69] “SES Selects Arianespace to Launch EAGLE-1 Satellite for Europe’s Quantum Cryptography,” SES, 09 11 2022. [Online]. Available: https://www.ses.com/press-release/ses-selects-arianespace-launch-eagle-1-satellite-europes-quantum-cryptography. [Accessed 12 04 2024].

[70] European Space Agency, “Quantum encryption to boost European autonomy,” 22 09 2022. [Online]. Available: https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Quantum_encryption_to_boost_European_autonomy. [Accessed 02 05 2024].

[71] ETSI, "Quantum Key Distribution," European Telecommunications Standards Institute, [Online]. Available: https://www.etsi.org/technologies/quantum-key-distribution. [Accessed 13 04 2024].

[72] ETSI, "INDUSTRY SPECIFICATION GROUP (ISG) ON QUANTUM KEY DISTRIBUTION (QKD)," European Telecommunications Standards Institute, [Online]. Available: https://www.etsi.org/committee/1430-qkd. [Accessed 13 04 2024].

[73] J. Śliwa and K. Wrona, "Quantum computing application opportunities in military scenarios," in *NATO Science and Technology Organisation - INTERNATIONAL CONFERENCE ON MILITARY COMMUNICATION AND INFORMATION SYSTEMS (ICMCIS)*, Skopje, North Macedonia, 2023.

[74] "The Warfare Development Agenda," NATO, [Online]. Available: https://www.act.nato.int/warfare-development-agenda/.

[75] "NATO Warfighting Capstone Concept," NATO Allied Command TRansformation (ACT), 2021. [Online]. Available: https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/. [Accessed 17 04 2024].

[76] S. Erwin, "Pentagon sees quantum computing as key weapon for war in space," SpaceNews, 15 07 2018. [Online]. Available: https://spacenews.com/pentagon-sees-quantum-computing-as-key-weapon-for-war-in-space/. [Accessed 01 08 2023].

[77] J. Prisco, "NATO Leads The Way With QKD While U.S. Lags," Forbes, 08 03 2024. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2024/03/08/nato-leads-the-way-with-qkd-while-us-lags/. [Accessed 02 05 2024].

[78] L. Pupillo , A. Ferreira, V. Lipiainen and C. Polito, "Quantum Technologies and Cybersecurity: Technology, Governance and Policy Challenges," Centre for European Policy Studies Task Force, 06 12 2023. [Online]. Available: https://www.ceps.eu/ceps-publications/quantum-technologies-and-cybersecurity/. [Accessed 31 01 2024].

[79] W. Rjaibi, S. Muppidi and M. O'Brien, "Wielding a double-edged sword: Preparing cybersecurity now for a quantum world," IBM Institute for Business Value, 07 2018. [Online]. Available: https://www.ibm.com/downloads/cas/5VGKQ63M. [Accessed 31 01 2024].

[80] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe and S. Lloyd, "Quantum machine learning," Nature, 14 09 2017. [Online]. Available: https://doi.org/10.1038/nature23474. [Accessed 02 05 2024].

[81] "Chinese Threats in the Quantum Era," Booz Allen Hamilton, 2021. [Online]. Available: https://www.boozallen.com/expertise/analytics/quantum-computing/chinese-cyber-threats-in-the-quantum-era.html. [Accessed 02 05 2024].

[82] European Commission, “Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography,” 11 04 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography#:~:text=This%20Commission%20Recommendation%20encourages%20Member,States%20and%20their%20public%20sectors.. [Accessed 07 05 2024].

[83] U.S. Department of Homeland Security, “Post-Quantum Cryptography,” 2022. [Online]. Available: https://www.dhs.gov/quantum. [Accessed 16 02 2024].

[84] Committee on National Security Systems, “Advisory Memorandum: Use of Public Standards for the Secure Sharing of Information among National Security Systems,” 07 2015. [Online]. Available: https://cryptome.org/2015/08/CNSS_Advisory_Memo_02-15.pdf. [Accessed 31 01 2024].

[85] “Post-Quantum Cryptography Standardization,” NIST, 05 06 2024. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization. [Accessed 07 05 2024].

[86] National Security Agency/Central Security Service, “Announcing the Commercial National Security Algorithm Suite 2.0,” National Security Agency, Cybersecurity Advisory, 07 09 2022. [Online]. Available: https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/. [Accessed 06 05 2024].

[87] J. Dargan, “15 Leading Quantum Computing Countries With National Initiatives,” The Quantum Insider, 29 04 2021. [Online]. Available: https://thequantuminsider.com/2021/04/29/leading-quantum-computing-countries/. [Accessed 03 05 2024].

[88] E. Parker, D. Gonzales, A. K. Kochhar, S. Litterer, K. O'Connor, J. Schmid, K. Scholl, R. Silberglitt, J. Chang, C. A. Eusebi and S. W. Harold, “An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology,” RAND Corporation, 02 02 2022. [Online]. Available: https://www.rand.org/pubs/research_reports/RRA869-1.html. [Accessed 09 04 2024].

[89] “Post-Quantum Cryptography,” NIST, 09 05 2024. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography. [Accessed 10 05 2024].

[90] “Quantum Technology Monitor,” McKinsey&Company, 2023. [Online]. Available: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20technology%20sees%20record%20investments%20progress%20on%20talent%20gap/quantum-technology-monitor-april-2023.pdf.

[91] Quantum Internet Alliance, “D4.1 Quantum Applications and Use Case Report,” 17 05 2021. [Online]. Available: https://quantuminternetalliance.org/wp-content/uploads/sites/6/2022/05/D4.1-Quantum-Applications-and-Use-Case-Report.pdf. [Accessed 12 04 2024].

[92] “WILL CHINA BECOME A TECH SUPERPOWER?,” China-Britain Business Council, 22 01 2021. [Online]. Available: https://www.cbbc.org/news-insights/will-china-become-tech-superpower. [Accessed 01 08 2023].

[93] “IBM Launches $100 Million Partnership with Global Universities to Develop Novel Technologies Towards a 100,000-Qubit Quantum-Centric Supercomputer,” IBM, 21 05 2023. [Online]. Available: https://newsroom.ibm.com/2023-05-21-IBM-Launches-100-Million-Partnership-with-Global-Universities-to-Develop-Novel-Technologies-Towards-a-100,000-Qubit-Quantum-Centric-Supercomputer. [Accessed 03 05 2024].

[94] A. Wilkins, “Google launches $5m prize to find actual uses for quantum computers,” New Scientist, 04 03 2024. [Online]. Available: https://www.newscientist.com/article/2420137-google-launches-5m-prize-to-find-actual-uses-for-quantum-computers/. [Accessed 03 05 2024].

[95] “Microsoft spending big to build quantum computer,” The Business Times, 21 11 2021. [Online]. Available: https://www.businesstimes.com.sg/startups-tech/technology/microsoft-spending-big-build-quantum-computer. [Accessed 06 05 2024].

[96] A. Mohn, M. Pronk and T. Timmerman, “Quantum computing risks and opportunities: how to become post-quantum ready,” Compact, 2023. [Online]. Available: https://www.compact.nl/articles/quantum-computing-risks-and-opportunities-how-to-become-post-quantum-ready/. [Accessed 05 09 2023].

[97] T. Attema, J. D. Duarte, V. Dunning, M. Lequesne, W. v. d. Schoot and M. Stevens, “Het PQC-migratie handboek,” Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 03 2023. [Online]. Available: https://www.aivd.nl/documenten/publicaties/2023/04/04/pqc-migratie-handboek. [Accessed 05 09 2023].

[98] M. Swayne, “Russian Scientists Expect A 50-Qubit Quantum Computer By End Of 2024,” The Quantum Insider, 24 02 2024. [Online]. Available: https://thequantuminsider.com/2024/02/24/russian-scientists-expect-a-50-qubit-quantum-computer-by-end-of-2024/#:~:text=Russian%20Scientists%20Expect%20a%2050%2DQubit%20Quantum%20Computer%20by%20End%20of%202024,-National%2C%20Research&text=A%20Russian%20sc. [Accessed 28 04 2024].

[99] "REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a framework for ensuring a secure and sustainable supply of critical raw materials and amending Regulations (EU) 168/2013, (EU) 2018/858, 2018/1724 and (EU) 2019/1020," European Commission, 16 03 2023. [Online]. Available: https://eur-lex.europa.eu/resource.html?uri=cellar:903d35cc-c4a2-11ed-a05c-01aa75ed71a1.0001.02/DOC_1&format=PDF. [Accessed 23 04 2024].

[100] E. Benson and T. Denamiel, "China's New Graphite Restrictions," Centre for Strategic & International Studies, 23 10 2023. [Online]. Available: https://www.csis.org/analysis/chinas-new-graphite-restrictions. [Accessed 24 02 2024].

[101] T. W. Edgar and D. O. Manz, in *Research Methods for Cybersecurity,* Cambridge, Elsevier, 2017.

[102] J. M. Converse, "Survey Research in the United States. Roots and Emergence 1890-1960.," University of California Press, 1987. [Online]. Available: https://doi.org/10.4324/9781315130491, https://www.science.org/doi/10.1126/science.240.4855.1057.

[103] D. Madrigal and B. McClain, "Strengths and Weaknesses of Quantitative and Qualitative Research," UXmatters, 03 09 2012. [Online]. Available: https://www.uxmatters.com/mt/archives/2012/09/strengths-and-weaknesses-of-quantitative-and-qualitative-research.php. [Accessed 04 01 2024].

[104] S. Jamieson, "Likert scale," Britannica, 31 10 2023. [Online]. Available: https://www.britannica.com/topic/Likert-Scale. [Accessed 05 01 2024].

[105] D. Gallego and S. Bueno, "Exploring the application of the Delphi method as a forecasting tool in Information Systems and Technologies research," 28 07 2014. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/09537325.2014.941348. [Accessed 24 11 2023].

[106] A. Joshi, S. Kale, S. Chandel and D. K. Pal, "Likert Scale: Explored and Explained," 01 2015. [Online]. Available: https://www.researchgate.net/publication/276394797_Likert_Scale_Explored_and_Explained. [Accessed 05 01 2024].

[107] K. Kauko and P. Palmroos, "The Delphi method in forecasting financial markets— An experimental study," ScienceDirect, 2014. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0169207013001489. [Accessed 23 11 2023].

[108] R. L. Custer, J. A. Scarcella and B. R. Stewart, "JVTE v15n2 - The Modified Delphi Technique - A Rotational Modification," 1999. [Online]. Available: https://scholar.lib.vt.edu/ejournals/JVTE/v15n2/custer.html. [Accessed 25 11 2023].

[109] A. Perera, “Hawthorne Effect: Definition, How It Works, And How To Avoid It,” SimplyPsychology, 13 02 2024. [Online]. Available: https://www.simplypsychology.org/hawthorne-effect.html. [Accessed 02 04 2024].

[110] O. Ingram, “What are Demand Characteristics, How do they Affect Participants?,” Research Prospect, 29 08 2023. [Online]. Available: https://www.researchprospect.com/what-are-demand-characteristics/. [Accessed 04 02 2024].

[111] L. Danilas, “NATO's Quantum Future,” NATO Innovation and Technology Magazine, 12 2023. [Online]. Available: https://issuu.com/globalmediapartners/docs/nitech10?fr=xKAE9_zU1NQ. [Accessed 12 03 2024].

[112] P. R. Allison , “'Quantum memory breakthrough' may lead to a quantum internet,” Live Science, 26 02 2024. [Online]. Available: https://www.livescience.com/technology/communications/quantum-memory-breakthrough-may-lead-to-a-quantum-internet. [Accessed 09 05 2024].

# Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Laura Danilas

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "The Impact of Quantum Technologies on NATO's Security and Defence Posture", supervised by Adrian Venables and Joanna Sliwa
    1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
    1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

12.05.2024

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

## Appendix 2 – Survey

The survey can be found at the following link: https://docs.google.com/forms/d/e/1FAIpQLSfieXFeA70sllW4QhyJcVXwfHFr_Bq4cUh_3SIDhXtcvsg6Tw/viewform

# Quantum Technologies

The following survey is being conducted by Laura Danilas, who is an MSc student studying Cybersecurity at the Tallinn University of Technology and an intern at the NATO Cyber Security Centre. The answers will be used for a Master's thesis research. The aim of the survey is to analyse the development and state of the art of quantum technologies within NATO member states.

The questionnaire consists of 34 statements that need to be evaluated according to the Likert scale [1]. Every statement has a comments section. At the end of every statement, you are encouraged to give as many comments and insights as possible. This will help the author to draw better conclusions and make this research as useful as possible.

Your response to the survey is completely voluntary. You can withdraw from the study at any time. The information gathered will be used solely for this MSc thesis and individual responses will not be given to any third party. The data collected will be presented anonymously, but the name of the respondent is required so that the author can ask additional questions or clarifications about the replies provided if necessary.

[1] A Likert scale is used to measure opinions, attitudes or behaviours – https://www.scribbr.com/methodology/likert-scale/

* Indicates required question

Please tick the box provided to show your consent to be part of the research.

☒I give my consent to be part of the research.

Please write your name.

Your answer

Who is your current employer?

Your answer

What is your current job position?

Your answer

**1. Quantum technologies (QT) will affect the future of cybersecurity by creating opportunities. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

*If you answered strongly agree/agree, then what kind of opportunities QT will bring?*

Your answer

**2. QT will improve the cybersecurity capabilities of NATO. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**3. QT will affect the future of cybersecurity by increasing the capability of threat actors. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer. *If you answered strongly agree/agree, then what kind of threats QT will bring?*

Your answer

**4. "Harvest now, decrypt later" [2] attacks are already a threat to NATO. ***

[2] Harvest now, decrypt later. The threat refers to a proactive approach taken by potential adversaries who compromise systems to collect encrypted data today with the intention of decrypting it in the future when quantum computers are powerful enough to break existing encryption methods.

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**5. "Harvest now, decrypt later" attacks are not a threat to NATO at the moment. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**6. QT have potentially disruptive implications, which can degrade NATO's ability to deter and defend. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**7. NATO should invest in QT now. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer. *If you answered strongly agree/agree, then which technologies NATO should invest in and when?*

Your answer

**8. NATO should keep track of what is currently being developed in terms of QT. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**9. NATO should wait and invest in QT when the technology is mature. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**10. NATO could effectively use QT in its military operations by as early as 2030. ***

*NOTE: According to NATO 2030 framework, NATO should preserve its edge in seven disruptive technologies, including quantum-enabled technologies.*

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer. *If you do not agree with the statement, what should be the timeframe then?*

Your answer

**11. NATO should increase the number of quantum companies taking part in DIANA [3] initiatives. ***

*NOTE: Right now, 6 out of 44 are quantum companies.*

[3] NATO's Defence Innovation Accelerator for the North Atlantic. A NATO body working with leading researchers and entrepreneurs across the Alliance, helping them develop technologies to keep NATO populations safe and secure. With dozens of accelerator sites and test centres across the Alliance, DIANA brings together universities, industry and governments to work with start-ups and other innovators to solve critical defence and security challenges. DIANA focuses on two main objectives – support for technology and business development and adoption of those technologies. DIANA aims to help the companies with solving the gap between technology demonstration and its transition into products ready for use. Read more here https://issuu.com/globalmediapartners/docs/nitech10?fr=xKAE9_zU1NQ, page 40.

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**12. In order to produce QT-based solutions suitable for military purposes, the industry needs input [4] from NATO member states. ***

[4] Military personnel provide input on the challenges and specific needs.

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**13. In order to produce QT-based solutions suitable for military purposes, input from NATO member states for the industry is not necessary. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**14. NATO should develop a process for supporting transition of QT from the lab to the operational environment. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**15. A process especially focused on the creation of QT applications in the military domain should be established. ***

*NOTE: Process focused on integrating considerations of quantum technologies' application in the implementation of NATO's operational concepts, defence planning cycles, capability development cycles, and standardisation efforts.*

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**16. A process specifically focused on creating QT applications in the military domain is unnecessary. Commercial drive will be sufficient to fulfil the capability gap. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**17. In order to increase the Technology Readiness Level (TRL) of QT that have potential to create strategic advantage, the most important aspect for NATO is cooperation with academia. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**18. In order to increase the TRL of QT that have potential to create strategic advantage, the most important aspect for NATO is cooperation with industry. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**19. Companies implementing Quantum Resistant [5] solutions will be ready with mature products not sooner than before 2030. ***

[5] Quantum Resistant. Quantum resistant algorithms are not prone to the cryptanalytic attack by a quantum computer. In particular, quantum resistant algorithms have been selected in the NIST (National Institute of Standards and Technology) Post-Quantum Cryptography Standardization Project and currently undergo the process of standardization; https://csrc.nist.gov/projects/post-quantum-cryptography.

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**20. Post-quantum cryptography when it becomes available is the best mitigation measure to become quantum safe. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**21. Post quantum cryptography using a hybrid approach [6] is the best mitigation measure to become quantum safe when it becomes available. ***

[6] Hybrid approach. Schemes that combine post-quantum and traditional algorithms for key establishment or digital signatures are often called hybrids. https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**22. Quantum Key Distribution (QKD) [7] is the best mitigation measure to become quantum safe, although it is not sufficiently mature yet. ***

[7] Quantum Key Distribution. QKD is key exchange mechanism using quantum properties (like entanglement), proven to provide theoretical security that cannot be broken by mathematical advances or by the quantum computer.

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**23. Quantum communications will provide a significant improvement in secure communications. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**24. NATO should implement an equitable transition of cryptographic systems to quantum-safe cryptography by 2030. ***

*NOTE: According to NATO 2030 framework, NATO should preserve its edge in seven disruptive technologies, including quantum-enabled technologies.*

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer. *If you do not agree with the statement, what should be the timeframe then?*

Your answer

**25. Every NATO nation should have its own quantum strategy, aligned with NATO's Quantum Strategy. ***

*NOTE: NATO released its first ever quantum strategy in January 2024.*

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**26. Every NATO nation should not have its own quantum strategy, NATO Quantum Strategy is enough. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**27. NATO nations could offer their quantum computer resources for NATO operations. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**28. NATO should create a Quantum Centre of Excellence that can speed up the development of quantum technologies tailored to military applications and promote the exchange of ideas among military personnel and Subject Matter Experts. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**29. NATO should broker opportunities made possible by QT with industry, governments, and end users, fostering scale up and adoption of QT to accelerate the development of QT-based military applications. One example is the development of the Transatlantic Quantum Community [8]. ***

[8] NATO Transatlantic Quantum Community. NATO has a Transatlantic Quantum Community to strategically engage with government, industry and academia from across its innovation ecosystems. It was established in order to create certain conditions for cooperation, fostering a closer cooperation among NATO member states, and a resilient quantum ecosystem that extends beyond availability of appropriate funding.

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**30. NATO should focus its investments on building a Fault-Tolerant Quantum Computer (FTQC [9]). ***

[9] Fault-Tolerant Quantum Computer. Computer that is designed to handle errors that naturally occur in quantum computations due to environmental factors or imperfections in the hardware. It employs error correction techniques to maintain the integrity of quantum information and ensure accurate results.

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer. *If you do not agree that this is the main line for investment, where should NATO focus its investments then (regarding DOTMLPF-I [10])?*

[10] DOTMLPF-I. Doctrine, Organisation, Training, Materiel, Leadership&Education, Personnel, Facilities and Interoperability. It is a framework used by military planners to assess and analyze various aspects of a system, process, or capability.

Your answer

**31. One of the biggest issues regarding the development of QT is the availability of enabling technologies and their ability to secure the supply chain [11]. ***

[11] Here the author means the ability to build the competence among NATO nations, so they could produce their technologies independently from the rest of the world. E.g. quantum computers require precise metrology tools, secure manufacturing capabilities of specialised manufacturing and cryogenics.

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**32. One of the biggest issues regarding the development of QT-based military capabilities on the NATO level relies on the challenge of attracting specialists in QT to work for NATO. ***

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer.

Your answer

**33. Regarding all EDTs [12], NATO should prioritise the efforts on the development and adoption of QT to gain strategic advantage. ***

*NOTE: For example, China invests already more than all NATO member states together.*

[12] Emerging Disruptive Technologies. NATO's innovation activities currently focus on nine priority technology areas, quantum is one of those.

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments to your answer. *What do you see as the most important part in this process? (Cooperation with academia, exercises, experiments, talent acquisition etc.)*

Your answer

**34. Regarding all EDTs, NATO should not prioritize efforts on the development and adoption of QT, but rather procure and deploy Commercial Off the Shelf (COTS [13]) equipment when ready. ***

[13] Commercial Off the Shelf. COTS refers to products or goods that are readily available in the market and not specifically developed for a particular customer or purpose.

Strongly disagree (1)

Disagree (2)

Neither agree nor disagree (3)

Agree (4)

Strongly agree (5)

Please provide comments for your answer.

Your answer